このサイトはAvast Business製品専用です。AVG Business製品に関する記事については、AVG Business ヘルプを参照してください。適切な場所にいても探している情報が見つからない場合は、 Avast Businessサポートに連絡してさらにサポートを受けてください。

CentOS 7 の推奨構成

この記事は以下に適用されます:

- Avast Business オンプレミス コンソール

Avast Business On-Premise Consoleを実行するために Docker を備えた CentOS 7 サーバーをインストールして構成する場合は、次の設定をお勧めします。

リモートアクセスとコントロールの設定

CentOS の最小インストールを実行する場合、安全なリモート アクセスを構成すると便利です。リモート ターミナル アクセスには、PuTTY などの SSH セッション ツールを使用することをお勧めします。このツールを使用するには、次のコマンドを使用して SSH サーバーを実行するように構成する必要もあります。`#vim /etc/ssh/sshd_config`

に次の変更を加えます`sshd_config`:

1. 「#LoginGrace Time 2m」を「LoginGrace Time 1m」に変更します。これにより、ログイン資格情報を入力する時間が 1 分に制限されます。必要に応じて、これを別の時間制限に設定できます。
2. 「#PermitRootLogin yes」を「PermitRootLogin no」に変更します。これにより、ユーザーが SvomSH 経由で直接 root ユーザーとしてログインできなくなります。ただし、sudo 権限を持つユーザーがログイン後に root に切り替えることは防げません (`sudo su -`)。
3. 「#MaxAuthTries 6」を「MaxAuthTries 2」に変更します。この行はすでに 2 に設定されている可能性がありますが、# 記号が削除されていることを確認してください。
4. 「#MaxSessions 10」を「MaxSessions 8」に変更します。この行はすでに 8 に設定されている可能性がありますが、# 記号が削除されていることを確認してください。
5. 「Subsystem s ftp /usr/libexec/openssh/sftp-server」を「#Subsystem sftp /usr/libexec/openssh/sftp-server」に変更します。この行はすでにコメントアウトされている可能性がありますが、ssh ログイン権限を持つすべてのユーザーが sftp アクセスできるようにするため、必ず # 記号でコメントアウトしてください。

さらに、ユーザーがルートに切り替えることを許可する「su」コマンドへのアクセスを制限するように PAM モジュールを構成する必要があります。

1. 次のコマンドを入力します。 `#vim /etc/pam.d/su`
2. 「#auth required pam_wheel.so use_uid」という行を見つけて、#記号を削除し、変更を保存します。

ssh デーモンを起動し、システムの起動時に自動的に起動するように設定する必要があります。そのためには、次のコマンドを入力します。

- `#systemctl enable sshd`
- `#systemctl start sshd`

最後に、安全性の低いリモート接続タイプを無効にする必要があります。これらはインストールすべきではありませんが、これらのコマンドで確認することができます。インストールされていない場合は、「操作を実行できませんでした」というエラーが表示されます。

- #systemctl disable telnet
- #systemctl disable rsh
- #systemctl disable rlogin
- #systemctl disable vsftpd

ssh がインストールされていれば、ssh ユーティリティを使用して、個人のデスクトップと CentOS サーバーの間でファイルを転送できます。これには、Bash シェル (Windows 10 および 11) を使用する必要があります。これは、scp コマンドを使用してサーバーとの間でファイルを転送するのに便利な方法です。

アクティブディレクトリ統合

CentOS 7 サーバーにログインするには、Active Directory の資格情報を使用することをお勧めします。ドメインに参加するには、次のものが必要です。

- 参加したい Active Directory ドメインのドメイン管理者の資格情報
- 参加する Active Directory ドメインの DNS サーバーの IP アドレス
- アクセスしたい検索ドメイン（追加するドメインや、オフィスにすでに存在する他の検索ドメインを含む）
- マシンが配置されているIPサブネット。これは10.160.22.128/25のような形式になります。スラッシュの後の数字はサブネットマスクです。

この情報を入手したら、すでにアクセスしている DNS サーバーと、参加する予定のドメインの DNS を追加するようにイーサネット接続を構成する必要があります。

イーサネット接続の設定

1. #nmtuiネットワークマネージャユーティリティを開くコマンドを入力します
2. ホスト名を設定する
    - これをネットワーク内で一意の名前に設定し、.localdomainを参加するドメインに変更して、[OK]を選択します。
3. 接続を編集する
    - エトが唯一のエントリーであるべきだ
4. プライマリイーサネットを選択します。ens192またはethoである必要があります。
5. IPv4 構成を表示
6. DNSサーバーの下で、追加を選択し、ドメインのDNS IPアドレスと、通常は自動的に取得される各DNSアドレスを入力します。
    - 通常自動的に取得されるアドレスのリストは、コマンドを入力することで見つけることができます#vim /etc/resolv.conf。DNS IPアドレスは、ディレクティブ「nameserver」に従います。
    - 一部のネットワーク ドライバーでは、最初の 3 つの DNS サーバー エントリのサポートのみが保証される場合があります。そのため、最初の 3 つのエントリには、ドメインの DNS、2 番目にオフィスの DNS、バックアップ DSN (オフィスのバックアップまたは 8.8.8.8) を含めるようにしてください。
7. 「検索ドメイン」で「追加」を選択し、必要な検索ドメインを入力します。
    - 自動的に取得された検索ドメインのリストは、コマンドを入力することで見つけることができます#vim /etc/resolv.conf。検索ドメインは、ディレクティブ「search」に従います。
8. 「自動的に接続する」と「すべてのユーザーが利用可能」の両方のチェックボックスに「x」が付いていることを確認して、「OK」をクリックします。
9. DNSエントリが入力した順序で使用されるようにするには、nmtuiを使用してアクセスできない接続設定の一部を編集する必要があります。次のコマンドを入力します。#vim /etc/sysconfig/network-scripts/ifcfg-<primary ethernet>
    - プライマリイーサネット名はens192またはethoで、編集したイーサネット接続の名前です。#nmtui

- 「PEERDNS=yes」を「PEERDNS=no」に変更します

10. [戻る]、[OK] の順に選択し、次のコマンドを入力してサーバーを再起動します。`#shutdown -r 0`

次に、Active Directory ドメインに参加するために必要ないくつかのパッケージをインストールする必要があります。

Active Directory ドメインに参加するために必要なパッケージのインストール

1. コマンドを実行する`#dnf -y install realmd sssd sssd-tools oddjob oddjob-mkhomedir adcli samba-common-tools avahi`
2. これが完了したら、次のファイルを編集します。
    1. `#vim /etc/avahi/avahi-daemon.conf`. 「[server)」見出しの下にある「domain-name=」行を見つけます。これがコメントアウトされている場合は、そのままにしておきます。コメントアウトされていない場合、つまり「local」に設定されている場合は、参加しようとしているドメイン名に変更します。
    2. `#vim /etc/nsswitch.conf`「hosts: files dns myhostname」という行を見つけます。順序を「dns files myhostname」に変更します。

次のコマンドを使用してドメインに参加できるようになります。

- `#realm discover domain Name`すると、以下の画像のような出力が表示されます。

```
[root@CentoOS7-flamm-local ~]# realm discover chlttraining.com
chlttraining.com
  type: kerberos
  realm-name: CHLTTRAINING.COM
  domain-name: chlttraining.com
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
```

- `#realm join -U domain Admin domain Name`すると、以下の画像のような出力が表示されます。

```
[dflamm@centos7-flamm ~]$ realm list
chlttraining.com
  type: kerberos
  realm-name: CHLTTRAINING.COM
  domain-name: chlttraining.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
  login-formats: %U
  login-policy: allow-permitted-logins
  permitted-logins:
  permitted-groups: domain admins
```

ドメインへの参加に成功したら、ドメイン ユーザー アクセスを構成する必要があります。まず、使いやすさを考慮して、完全修飾ドメイン名を必要としないドメイン ログインを設定する必要があります。

ドメインへの参加に成功したら、ドメイン ユーザー アクセスを構成する必要があります。まず、使いやすさを考慮して、完全修飾ドメイン名を必要としないドメイン ログインを設定する必要があります。

1. ファイルを編集する`#vim /etc/sssd/sssd.conf`
2. 「use_fully_qualified_names = True」を「use_fully_qualified_names = False」に変更して保存します。
3. 次のコマンドを入力します。 `#systemctl restart sssd`

次に、サーバーにログインできる Active Directory ユーザー グループを制限します。ドメイン管理者または特に管理者権限を与えたい別のグループに制限することをお勧めします。

1. コマンドを入力してください`#realm permit -g "user group"`
    - ユーザーグループ名は、ドメインに参加しているコンピュータからWindowsコマンドプロンプトに次のコマンドを入力することで見つけることができます: net group /domain。出力はすべてのグループのリストになります。
2. コマンドを入力してください`#visudo`
3. 「%wheel ALL=(ALL) ALL」という行を見つけて、その下に「%userl group ALL=(ALL) NOPASSWD: ALL」のような行を追加します。グループ名にスペースがある場合は、その前に「\」を付ける必要があります。これにより、選択したグループは su だけでなく sudo コマンドも使用できるようになり、必要に応じてルートに切り替えることができます。

上記が完了すると、サーバーを再起動してドメイン資格情報を使用して接続し、ログイン後にパスワードを再度要求されることなく root に切り替えることができるようになります。

セキュアFTP

Linux OS との間でのファイル転送を容易にするために、ファイル転送プロトコル サービスをインストールすることをお勧めします。標準の FTP ではすべての情報が暗号化や認証なしで送信されることに留意することが重要です。そのため、このガイドでは、暗号化とユーザー認証の両方を使用する安全な FTP サーバーの設定手順を説明します。

このガイドでは、OpenSSH の統合された sftp サーバー機能を使用して、sftp グループに追加したユーザーのみが sftp サーバーにアクセスできるように特別に設定しています。また、同時 ssh セッション数の制限は、sftp セッション数にも適用されることに注意してください。

sftp サーバーに接続するには、Filezilla などのユーティリティをワークステーションにダウンロードすることをお勧めします。また、sftp を使用する場合は、サーバー アドレスを必ず「`sftp://serverNameOrIP`」の形式で入力してください。また、sftp サーバーを追加したポートも入力する必要があるため、注意してください。このガイドではポート 22220 を使用します。

適切なユーザー アクセス制御を備えた安全な FTP サービスをインストールするには、まず、以前に設定した SSH サービスの 2 番目のインスタンスを作成して構成する必要があります。これを行うには、次のコマンドを使用します。

- `#groupadd sftp_users`
- `#mkdir /sftp`
- `#chown root:root /sftp`
- `#cp /etc/ssh/sshd{,-second}_config`
- `#vim /etc/ssh/sshd-second_config`

次に、次の操作を実行します。

1. 次の行を見つけて、その値が以下に示すとおりであることを確認します。存在しない場合は、「AcceptEnv」の行の下に追加します。
    - ポート 22220
    - Pidファイル /var/run/sshd-second.pid
    - プロトコル2
    - サブシステム sftp 内部 sftp
    - 許可グループ sftp_users

- ForceCommand 内部-sftp
- Chrootディレクトリ /sftp/%u
- 許可トンネル番号
- AllowAgentForwarding いいえ
- X11転送なし
- TcpForwarding を許可しない

2. 「Description=OpenSSH サーバーデーモン」を「Description=OpenSSH SFTP サーバーデーモン」に変更します。
3. 「After=network.target sshd-keygen.service」を「After=network.target network.target Auditd.service sshd.service」に変更します。
4. 「ExecStart=/usr/sbin/sshd -D $OPTIONS」を「ExecStart=/usr/sbin/sshd -D -f /etc/ssh/sshd-second_config $OPTIONS」に変更します。
5. ファイルを保存し、次のコマンドを実行します。
   - #semanage port -a -t ssh_port_t-p tcp 22220
   - #firewall-cmd --permanent --add-port=22220/tcp
   - #firewall-cmd --reload
   - #setsebool -P ssh_chroot_rw_homedirs on
   - #systemctl enable sshd-second
   - #systemctl start sshd-second
   - #shutdown -r

sftp サーバーを設定した後も、ログインできるようにする各ユーザーに対してアクセス権を付与する必要があります。 sftp アクセスを許可する各ユーザーに対して、次のコマンドを実行します。

- #usermod -aG sftp_users <userName>
- #mkdir /sftp/<userName>
- #mkdir /sftp/<userName>/sftp_dir
- #chown -R root:root /sftp/<userName>
- #chown -R <username> sftp_users /sftp/<userName>/sftp dir
- #chmod -R 755 /sftp/<userName>

ユーザーの sftp アクセスを取り消す必要がある場合は、次のコマンドを使用します#gpasswd -d <userName> sftp_users #rm -R /sftp/<userName>。

このセクションの他の記事:

CentOS 7 Linuxサーバーの準備

Linux に Docker Compose をインストールする

Linux にオンプレミス コンソールをインストールする

Linux での Docker の更新とアップグレード

Linux 上のオンプレミス コンソールの更新

Linux でのオンプレミス コンソール データベースのバックアップと復元

関連記事：

システム要求

ファイアウォールの要件

現在の場所: オンプレミス コンソール>コンソール管理 - *Linux* > *CentOS 7* の推奨構成