splunk>

Splunk 基本 1 ラボ実習

ラボ表記規則:

`[sourcetype=db_audit]` または `[cs_mime_type]` はソースタイプまたはフィールド名を指します。

備考: **ラボ作業が個人のコンピュータまたはバーチャルマシンで実施された場合、ラボ環境は提供されません。 運用環境でのラボ作業は決して実施しないでください。**

ラボモジュール 3 - Splunk Enterprise インストール

説明

このラボ実習では自身のラボ環境に Splunk Enterprise をインストールし、権限付ロールを持ったユーザーを作成します。

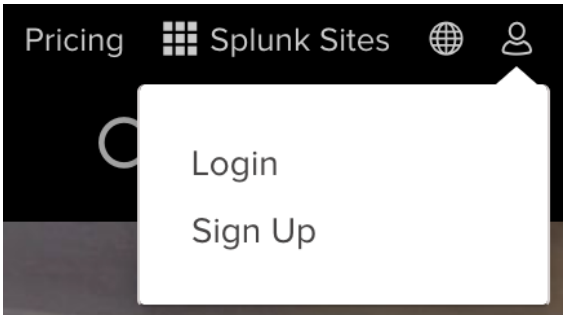
備考: **すべてのシステムやネットワークが同じとは限りません。 インストールで何らかのトラブルが生じた場合は、自身のオペレーティングシステム用の文書を確認してください。**

手順

シナリオ: あなたは最近 Buttercup Games のチームに Splunk 管理者として加わりました。 Splunk Enterprise をインストールし、ユーザー用アカウントを作成するように依頼されます。

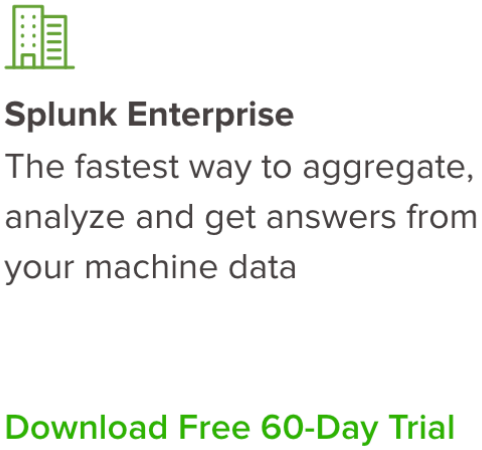
タスク 1: 自身のオペレーティングシステム用の Splunk Enterprise をダウンロードします。

1. ウェブブラウザで **http://splunk.com** を指定します。
2. 自身の splunk.com アカウントでログインするか、splunk.com ユーザーメニューの**ログイン**リンクを使用して新規アカウントを作成します。

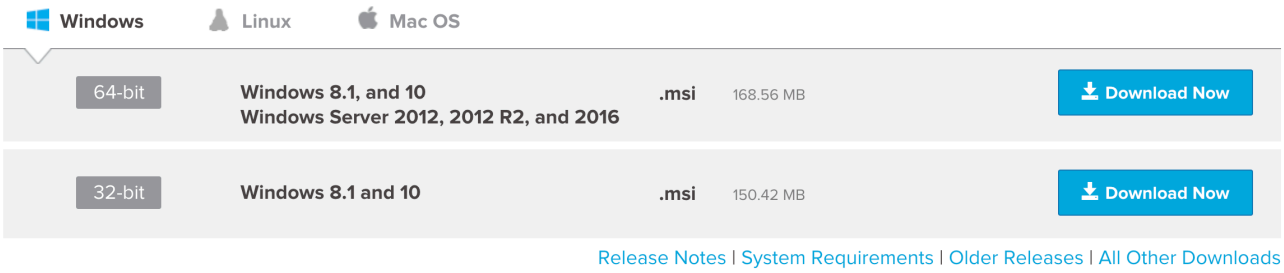


3. ログインしたら、インターフェースの右上にある緑の**無料 Splunk** ボタンをクリックします。

4. **Splunk Enterprise** から、**60 日無料トライアルダウンロード**リンクをクリックします。



5. タブを使って自身のオペレーティングシステムを選択し、アーキテクチャ用に**今すぐダウンロード**ボタンをクリックします。

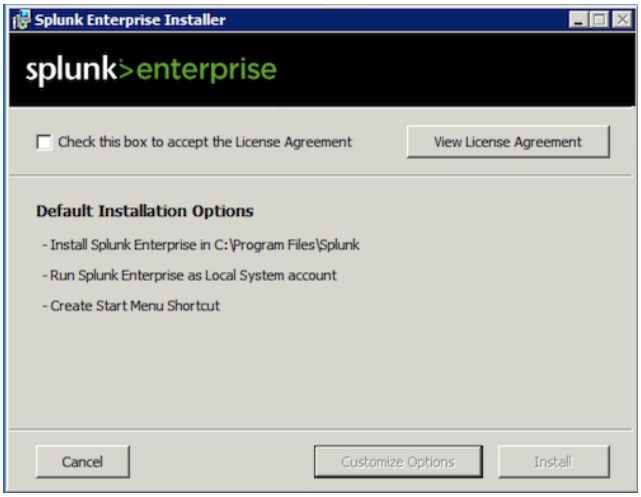


備考: Splunk Enterpriseをインストールするため、自身の環境に適合するタスクに進んでください。

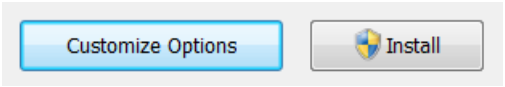
	Windows OS - タスク 2
	Linux OS - タスク 3
	Mac OS - タスク 4

タスク 2: Splunk Enterprise を Windows 環境でインストールします。

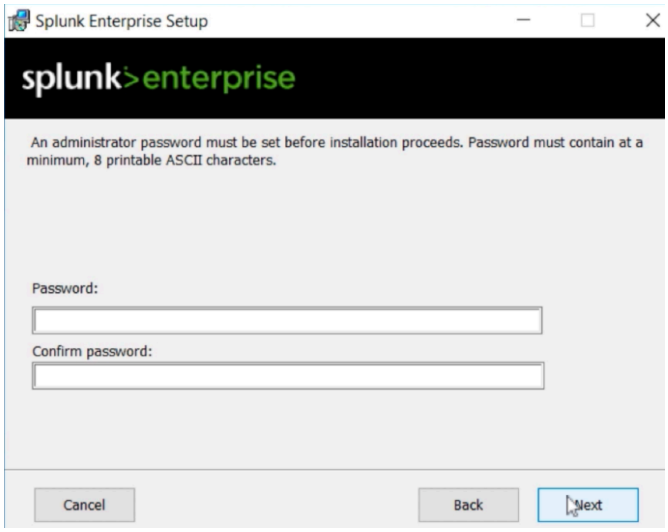
6. 前もってダウンロードした **splunk.msi ファイル**を見つけ、それをダブルクリックします。
7. インストーラーが作動し **Splunk Enterprise インストーラー**パネルを表示します。



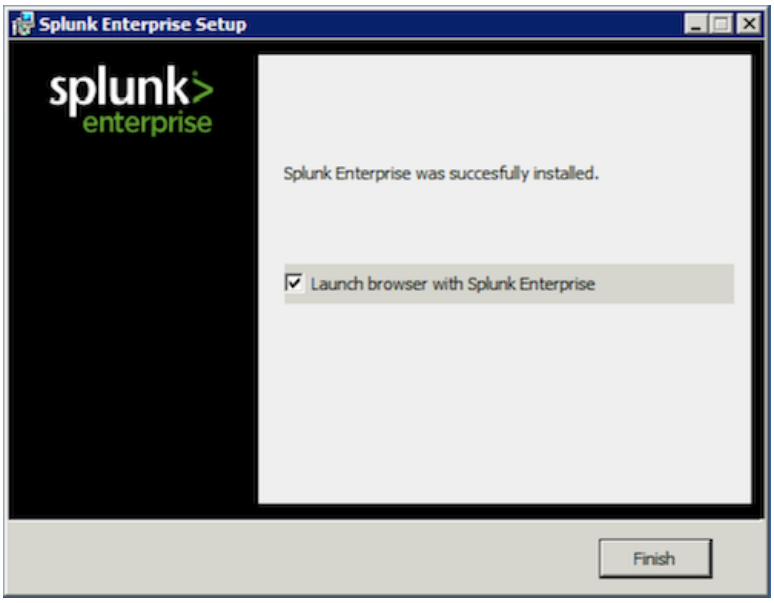
8. **ライセンス契約**ボタンをクリックしてライセンス契約を表示させ、**このボックスをチェックしてライセンス契約を承認**チェックボックスを使用してライセンス契約を承認します。
9. インストールをカスタマイズするボタンがありますが、このラボでは**インストール**ボタンをクリックしてデフォルトインストールオプションを使用します。



10. インストーラーから、管理者アカウントのパスワードを作成するように要求されます。



11. インストーラーがソフトウェアをインストールし、**インストール完了**パネルを表示します。



12. **Splunk Enterprise でブラウザを起動**チェックボックスがデフォルトで選択されます。 **終了**ボタンをクリックすると自身のデフォルトブラウザで Splunk Web が開きます。
13. タスク 5 に移動してラボを続けます。

タスク 3: Splunk Enterprise を Linux 環境でインストールします。

備考: このタスクではSplunk Enterpriseの.tgzアーカイブを使用します。

14. ターミナルウィンドウから、インストール中のサーバー上で、あらかじめダウンロードした **splunk.tgz** ファイルを含むディレクトリに移動します。
15. アーカイブをサーバーのルートディレクトリの **opt** フォルダに解凍します。

```
sudo tar xvzf splunk.tgz -C /opt
```

16. **bin** ディレクトリに **splunk** フォルダ内で移動します。

```
cd /opt/splunk/bin
```

17. **Splunk** を**ライセンス承認**引数のついた**開始**コマンドを使用して開始します。 任意で、**ライセンス承認**引数を省いてライセンス契約を読みます。

```
sudo ./splunk start --accept-license
```

18. 管理者アカウントのパスワードを作成するように要求されます。

```
新しいパスワードを入力してください:
```

19. **Splunk Enterprise** が前提条件と設定を確認します。 終了すると、**Splunk Web** の準備が整ったことを知らせるメッセージが表示されます:

```
Splunk web インターフェースは http://******:8000 です
```

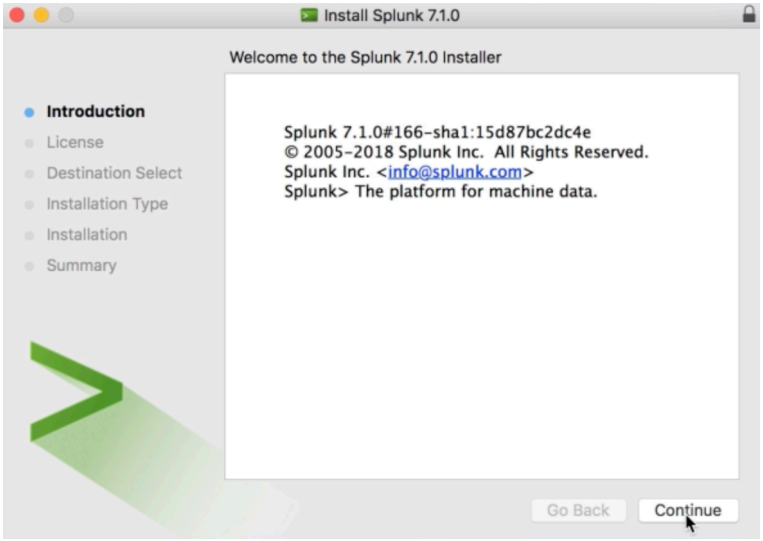
20. ブラウザウィンドウを開き、サーバーの IP アドレスまたはドメイン名をポート 8000 で指定します。
21. ブラウザで **Splunk Web** が確認できるようになります。

22. タスク 5 に移動してラボを続けます。

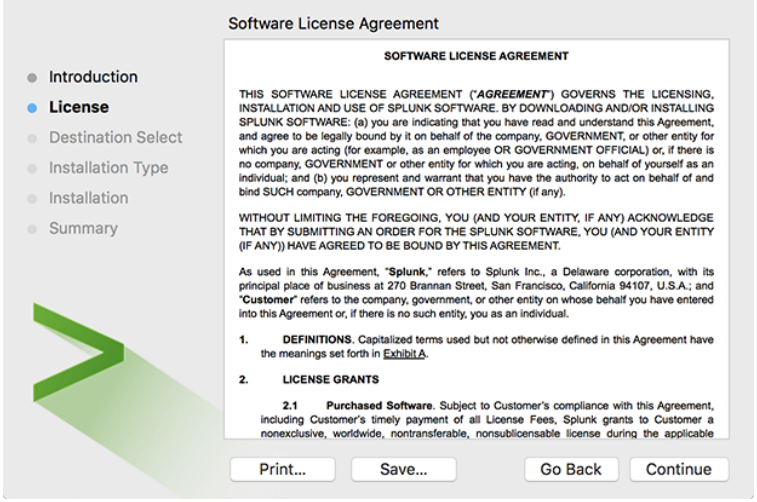
タスク 4: Splunk Enterprise を Mac 環境でインストールします。

23. 前もってダウンロードした **splunk.dmg ファイル**を見つけ、それをダブルクリックします。
24. Splunk インストーラーディスク 画像が開きます。
25. **Splunk インストール**アイコンをダブルクリックします。

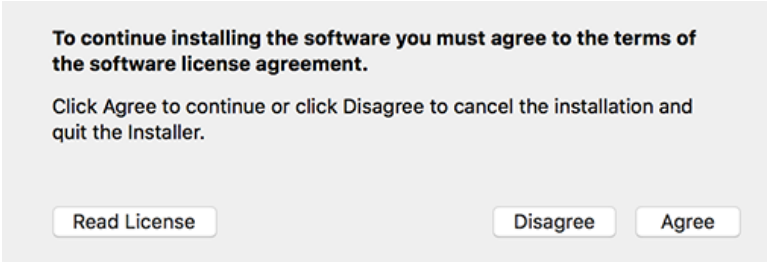
26. インストーラーが作動し **Splunk Enterprise インストーラー**パネルを表示します。



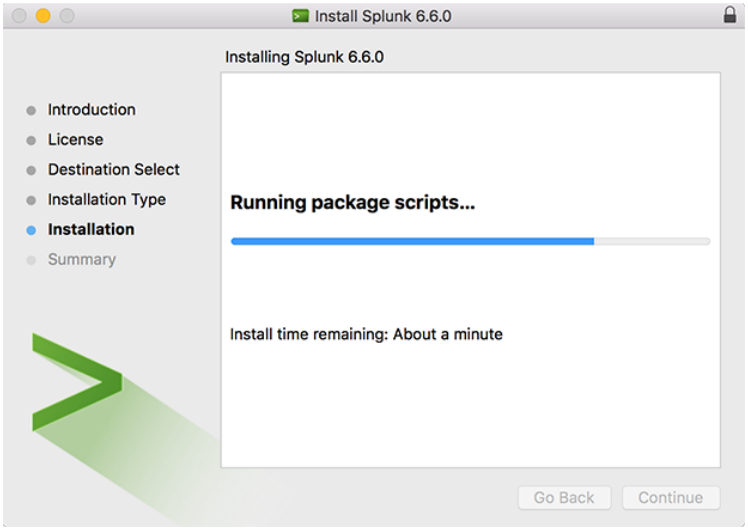
27. **継続**をクリックすると**ソフトウェアライセンス契約**が表示されます。



28. **継続**をクリックし、**同意**ボタンでライセンスを承認します。



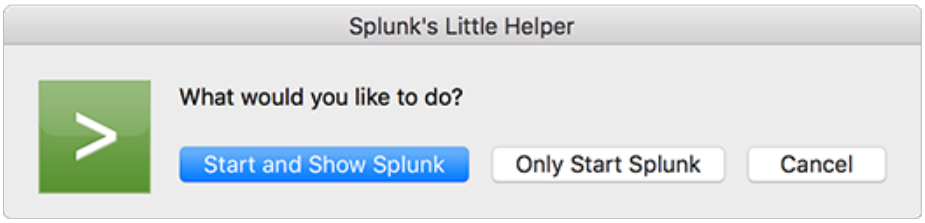
29. **インストール**ボタンをクリックするとインストールプロセスを開始します。



30. インストールされると、Splunk は **Splunk のリトルヘルパー**を開きます。 **OK** をクリックして Splunk がシステムで初期化できるようにします。
31. ターミナルウィンドウが開き、管理者アカウントのパスワードを作成するように要求されます。

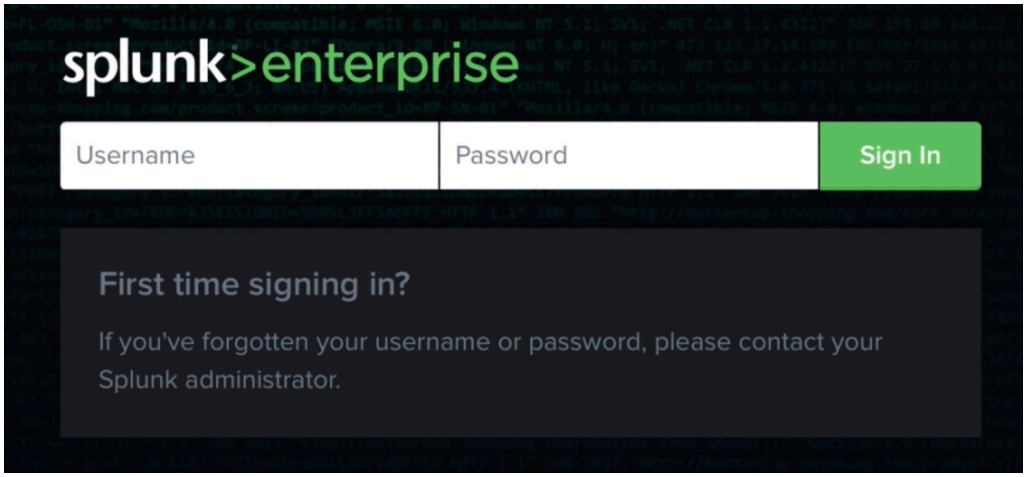
```
新しいパスワードを入力してください：
```

32. ターミナルウィンドウが閉じます。 Splunk のリトルヘルパーで**開始して Splunk を表示**ボタンをクリックします。Splunk はターミナルウィンドウを開き、Splunk を開始して Splunk Web をデフォルトブラウザに表示します。



タスク 5: Splunk Web にログインします。

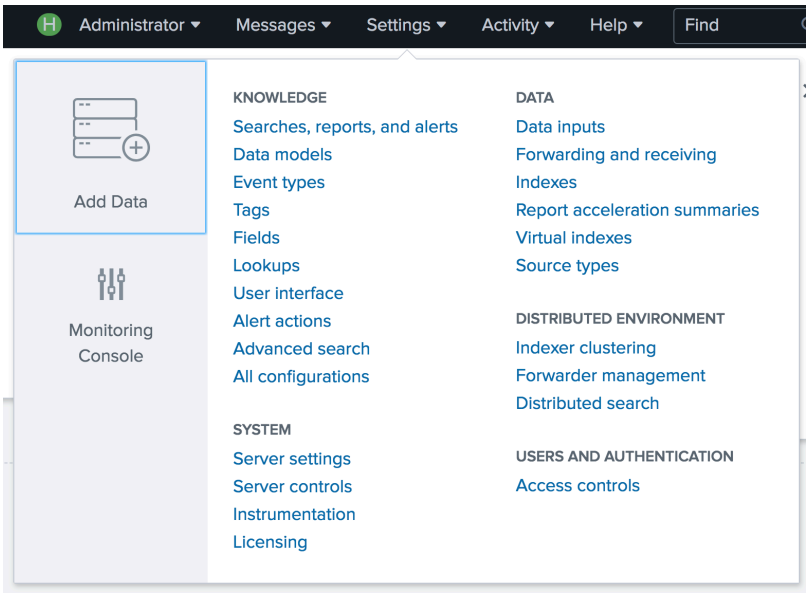
33. Splunk Web がブラウザで確認できない場合、**http://<ホスト名または IP アドレス>:8000** に移動してください。
34. **admin** のユーザー名とインストール中に作成したパスワードを使用して、管理者アカウントにログインします。



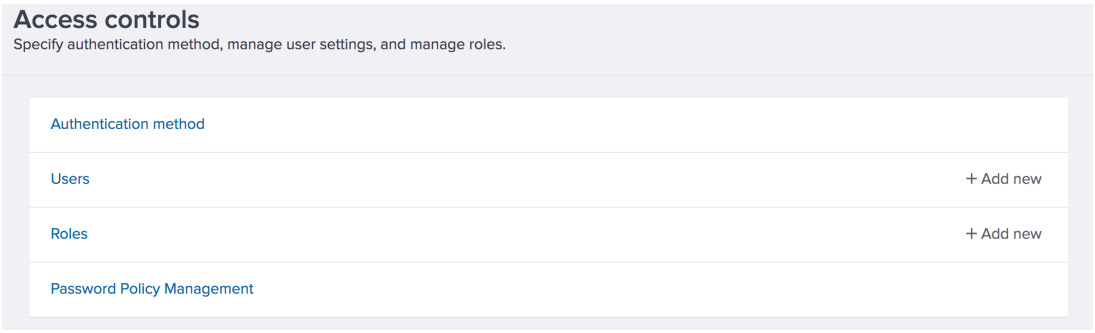
備考: パスワードを紛失した場合、Splunkサポートはその復元をヘルプすることはできません。

タスク 6: 権限付ロールを持ったユーザーを作成します。

35. Splunk バーから、**設定**メニューの**アクセス制御**を選択します。

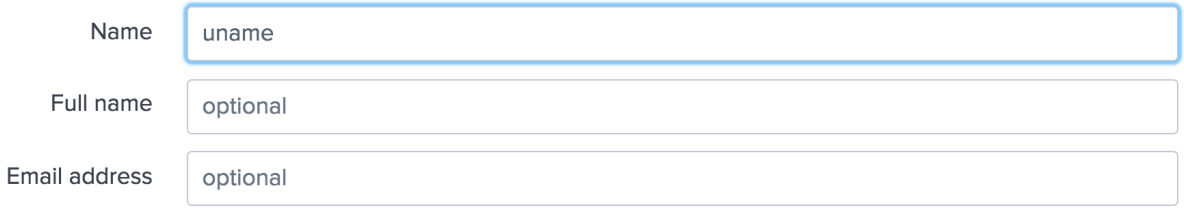


36. アクセス制御ページで**ユーザー**用**新規追加**.をクリックします。



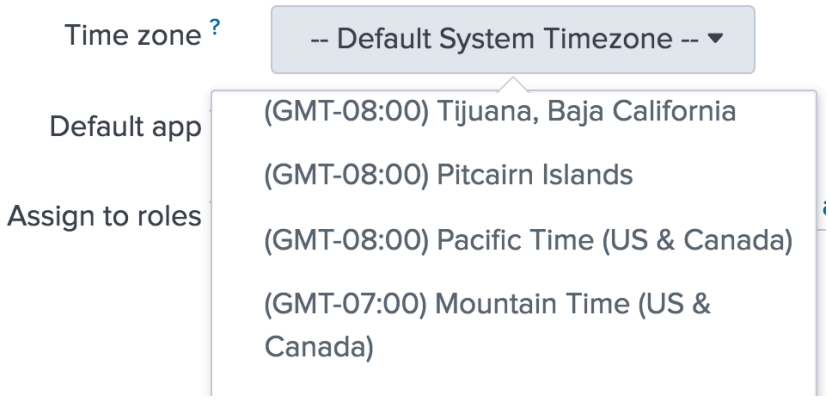
備考: このコースで使用するパワーユーザーアカウントを作成します。
自身のアカウントを作成したくない場合は、提案されたユーザー名およびパスワードを使用してください。
異なったユーザー名を作成すると、Splunkサポートはログイントラブルが生じた際サポートすることができません。

37. 「`uname`」を **Username** フィールドに入力します。

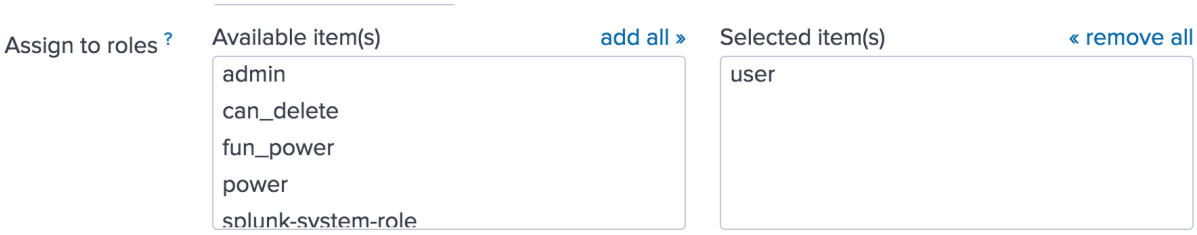


38. パスワードとパスワードの再入力に「`5p1unkbcup`」を入力します。

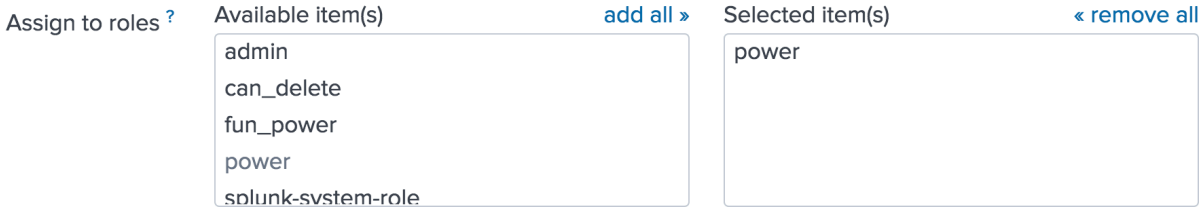
39. タイムゾーンを**タイムゾーン**ドロップダウンメニューから選択します。



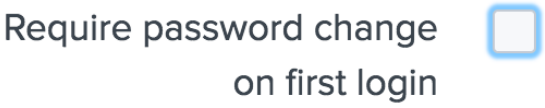
40. **ロールに割り当て**セクションで、**選択されたアイテム**から**ユーザー**アイコンをクリックして、リストから削除します。



41. **利用可能なアイテム**から**パワー**アイコンをクリックし、**選択されたアイテム**リストに追加します。



42. **初回ログイン時にパスワードの変更を要求**からチェックマークを削除して、**保存**をクリックします。



43. ユーザーが保存されると、ユーザー管理ページに戻ります。