LogicVein

Net LineDancer

ユーザマニュアル

目次

目次

目次

改訂履歴

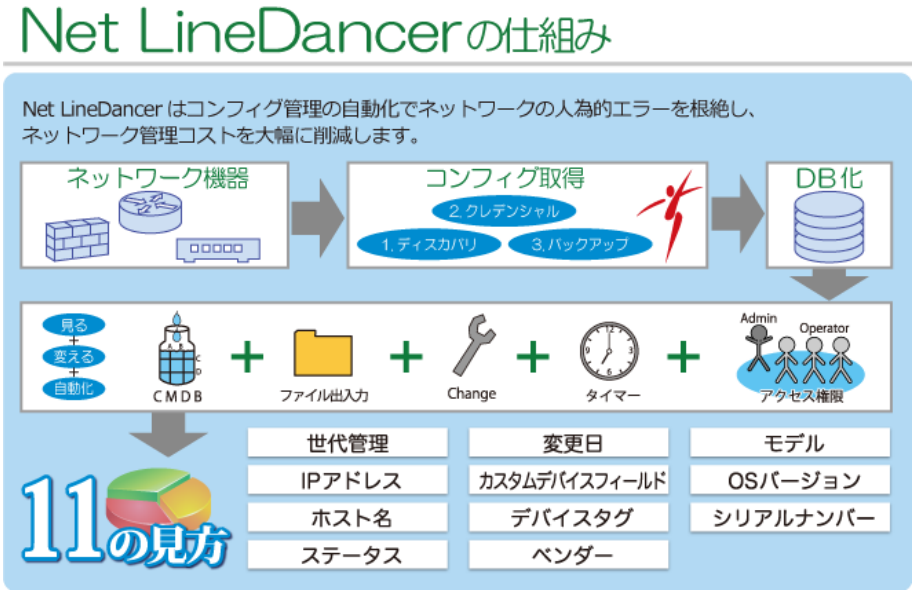
版数	発行日	改訂内容
第 1 版	2019 年 8 月 22 日	初版発行
第 2 版	2019 年 10 月 2 日	機能追加に伴い、説明および画像を修正
第 3 版	2019 年 11 月 25 日	承認機能を追加
第 4 版	2020 年 1 月 27 日	リビジョン更新に伴い、説明および画像を修正
第 5 版	2020 年 2 月 28 日	承認機能の仕様を変更
第 6 版	2020 年 3 月 31 日	コンプライアンスの説明と画像を修正
第 7 版	2021 年 3 月 30 日	推奨ブラウザの変更 アクティベーション手順オフライン環境を追加 使用ポートの変更と追加
第 8 版	2021 年 4 月 14 日	使用ポートの記載を修正
第 9 版	2021 年 4 月 26 日	システムバックアップ変更に関する注意を追加
第 10 版	2022 年 10 月 31 日	カスタムデバイスフィールドの記載と画像を修正 デバイスの EOS/EOL 管理機能を追加
第 11 版	2023 年 11 月 30 日	バルクチェンジの説明を更新
第 12 版	2024 年 2 月 7 日	バルクチェンジ機能の改善により更新
第 13 版	2024 年 3 月 11 日	動作環境を更新
第 14 版	2024 年 4 月 11 日	デプロイ手順に、Linux KVM / Nutanix AHV / AWS / Microsoft Azure を追加
第 15 版	2024 年 10 月 1 日	新機能を追加し、操作手順を追記
第 16 版	2025 年 1 月 27 日	新機能を追加（冗長機能、Allied JUNOS OS 配布）
第 17 版	2025 年 5 月 28 日	Playbook のノードを追加
第 18 版	2025 年 7 月 24 日	新機能を追加（クラウドアカウント）
第 19 版	2025 年 8 月 27 日	Playbook のノードを追加、Playbook 仕様変更に伴コンプライアンス機能の説明を更新
第 20 版	2025 年 10 月 1 日	デプロイ手順に Podman を追加、新機能追加に伴い画像の変更（Playbook）
第 21 版	2025 年 10 月 7 日	機能追加による画像変更（SNMP トラップのディスカバリ
第 22 版	2025 年 11 月 4 日	機能追加による変更（SNMP トラップのディスカバリ、モニターステータスレポート）
第 23 版	2025 年 12 月 5 日	Playbook の承認機能追加、履歴表示画面の構成変更に伴い説明を更新
第 24 版	2026 年 4 月 24 日	新機能を追加（SSH 秘密鍵認証、Playbook ノード（フィールド編集)）
第 25 版	2026 年 6 月 25 日	Playbook のノード構成変更に伴い説明を更新

1. はじめに

本書は、ネットワークコンフィギュレーション管理ソフトウェア「Net LineDancer」（以降、netLD と略します）のマニュアルです。netLD の各種設定や操作方法について説明します。

1.1 Net LineDancer とは

netLD は、ルータやスイッチなどのネットワーク機器の設定（コンフィギュレーション、インタフェース定義やアクセス制御リストなど）をバックアップ／世代管理するソフトウェアです。これによりインベントリ一覧リスト、プロパティの閲覧、コンフィギュレーションの比較、パスワードの変更、設定変更自動検知と NMS への通知など総合的なコンフィギュレーション管理を可能にし、効果的な運用管理を実現します。製品画面およびマニュアルは、ともに完全日本語対応であるだけでなく、ウィザードを多く利用できる GUI を提供し、初心者でも簡単に操作ができます。管理できる機種が多いマルチベンダー対応も大きな魅力のひとつです。



netLD の主な機能は、以下のとおりです。

主な機能

1. コンフィギュレーションバックアップ/世代管理
2. コマンドランナー
3. デバイス情報テキスト出力（タイムスタンプ付）
4. コンフィギュレーション復元（同一/別デバイス）
5. コンフィギュレーション文字列検索
6. IOS ファームウェア抽出/配布
7. show コマンド戻り値の取得/比較/テキスト出力
8. 実行ジョブの確認/リサイクル
9. ターミナルプロキシ機能
10. コンプライアンス機能
11. ユーザアクセスコントロール
12. MSP オペレーションズスイート
13. 完全日本語対応
14. ドラフトコンフィギュレーション/チェンジアドバイザ
15. 月額従量課金型のクラウドライセンス
16. Zero-Touch を日本初サポート
17. API 連携可

1.2 動作環境

netLD は、バーチャルアプライアンスとして提供され、以下のプラットフォームをサポートしています。

- VMware ESXi (バージョン 7.0 以上)
- Windows Hyper-V (Windows Server 2016 以降)
- Amazon Web Services
- Nutanix AHV
- Linux KVM
- Microsoft Azure

netLD を使用するには、次の環境が必要です。

項目	推奨	デフォルト	最小
ハードディスク	HDD1: 2.5 GB HDD2: 50 GB	HDD1: 2.5 GB HDD2: 50 GB	HDD1: 2.5 GB HDD2: 50 GB
HDD プロビジョニング	シン または シック	シン または シック	シン または シック
メモリ	8 GB 以上	16 GB	4 GB
CPU	仮想 CPU 8 個(コア) 以上	仮想 CPU 16 個(コア)	仮想 CPU 2 個(コア)

その他特記事項

※ HDD プロビジョニングタイプは、シン／シックのいずれのタイプもサポートされています。

■ブラウザ

Google Chrome（最新版）

Mozilla Firefox（最新版）

Microsoft Edge（最新版）

2. インストール

netLD のセットアップの流れは以下のとおりです。

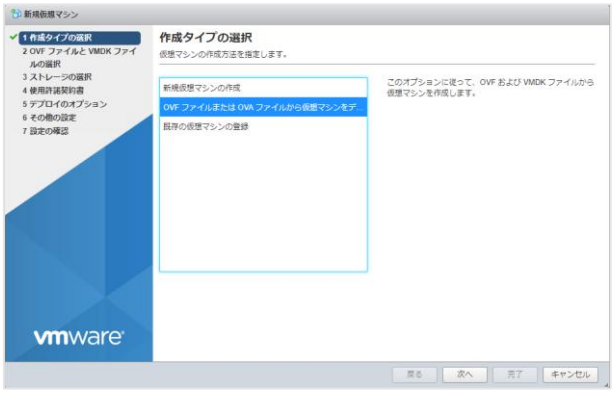
2.1 インストールする

2.1.1 VMware ESXi へのデプロイ

VMware ESXi へのデプロイ手順について説明します。ここでは ESXi 6.5 を使用した場合を例に説明します。

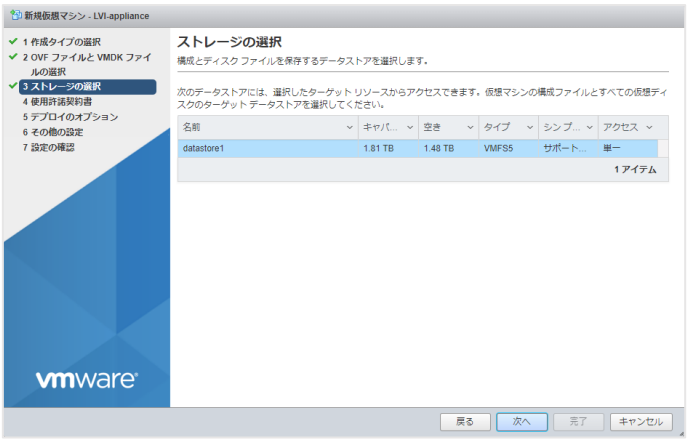
1. Web UI にログインし、仮想マシンから「仮想マシンの作成/登録」をクリックします。

2. 「OVF ファイルまたは OVA ファイルから仮想マシンをデプロイ」を選択し、「次へ」をクリックします。

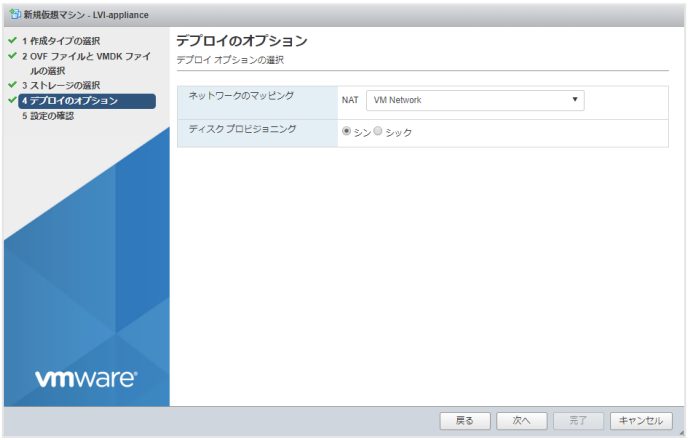


3. 任意の仮想マシン名を入力後、OVA ファイル「lvi-core-****-appliance.ova」をドラッグ・アンド・ドロップし「次へ」をクリックします。

4. ストレージを選択し「次へ」をクリックします。



5. デプロイするネットワークとディスクのプロビジョニングを選択し「次へ」をクリックします。



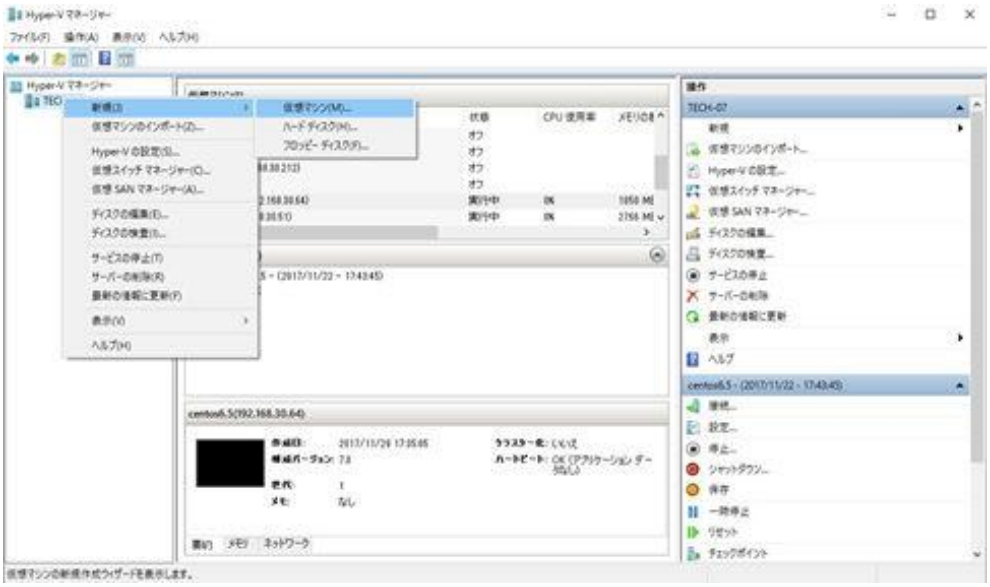
6. 「完了」をクリックします。

VMware ESXi へのデプロイは以上です。次に、デプロイした仮想マシンを起動しネットワーク設定をします。ネットワーク設定については、「2.2 ネットワークを設定する」を参照してください。

2.1.2 Windows Hyper-V へのデプロイ

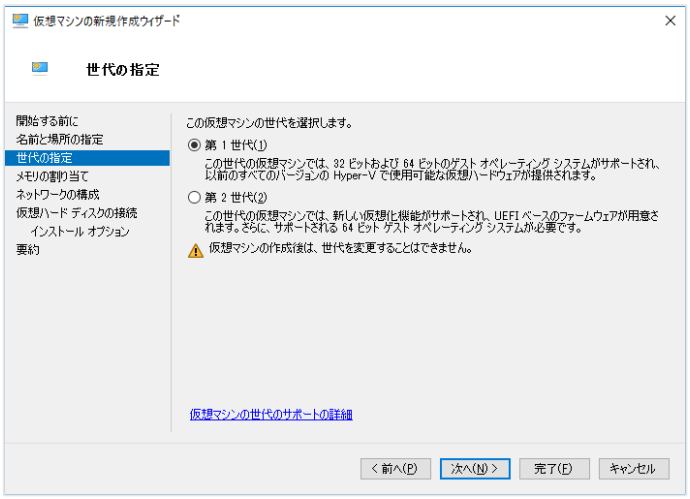
Windows Hyper-V へのデプロイ手順について説明します。ここでは Windows Server 2016 を使用した場合を例に説明します。

1. Hyper-V マネージャーを起動し、「操作」→「新規」→「仮想マシン」をクリックします。

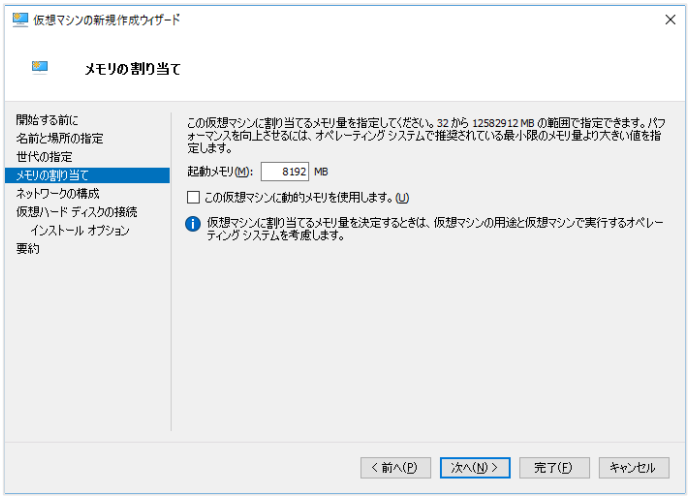


2. 仮想マシンの名前を入力し、「次へ」をクリックします。

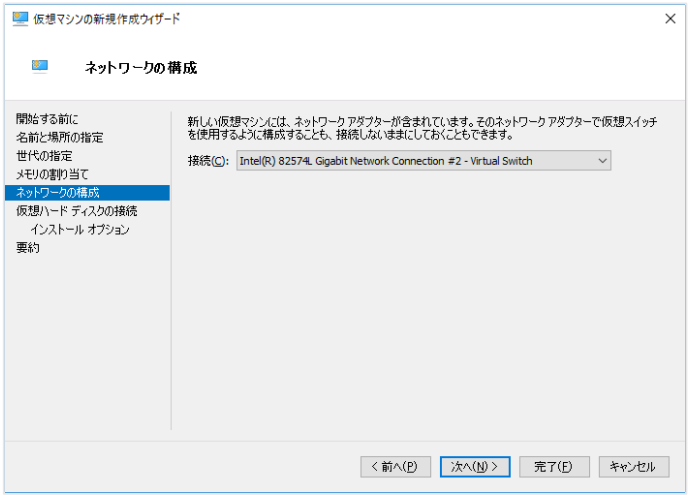
3. 「第 1 世代」を選択し、「次へ」をクリックします。



4. 起動メモリを設定し、「次へ」をクリックします。

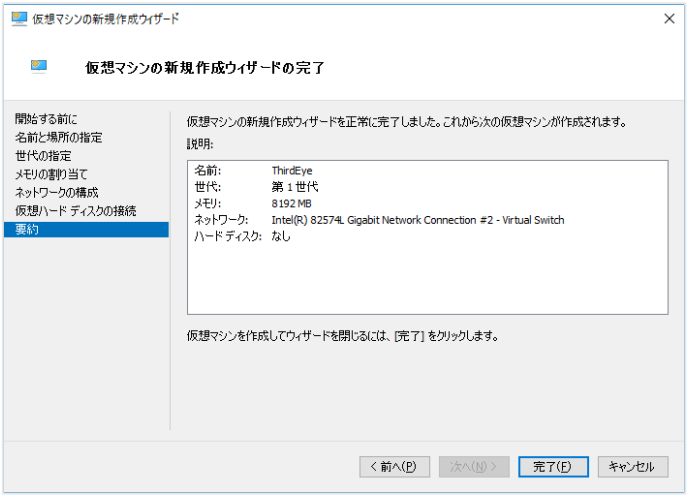


5. 接続先に使用する仮想スイッチを選択し、「次へ」をクリックします。



6. 「後で仮想ハードディスクを接続する」を選択し、「次へ」をクリックします。

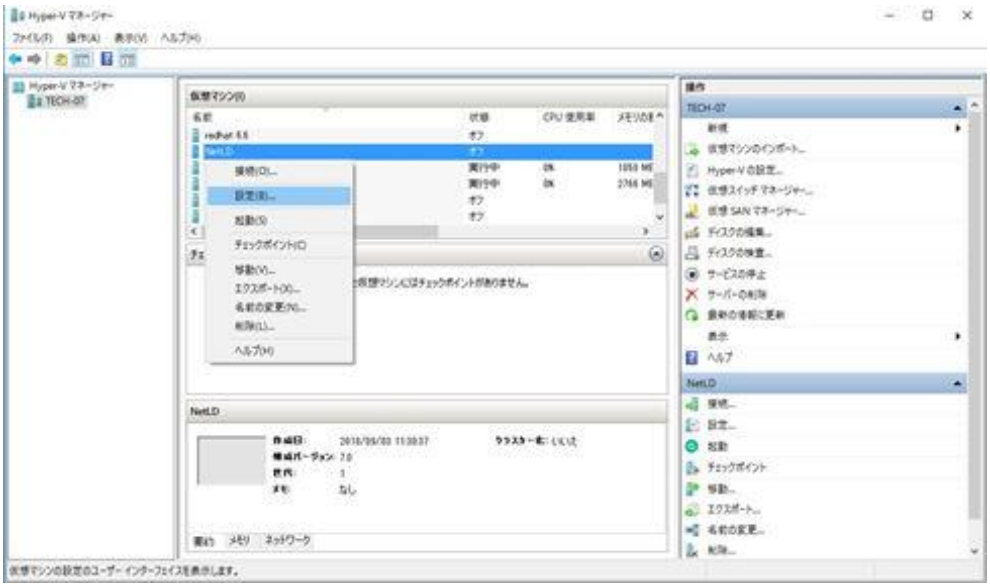
7. 「完了」をクリックします。



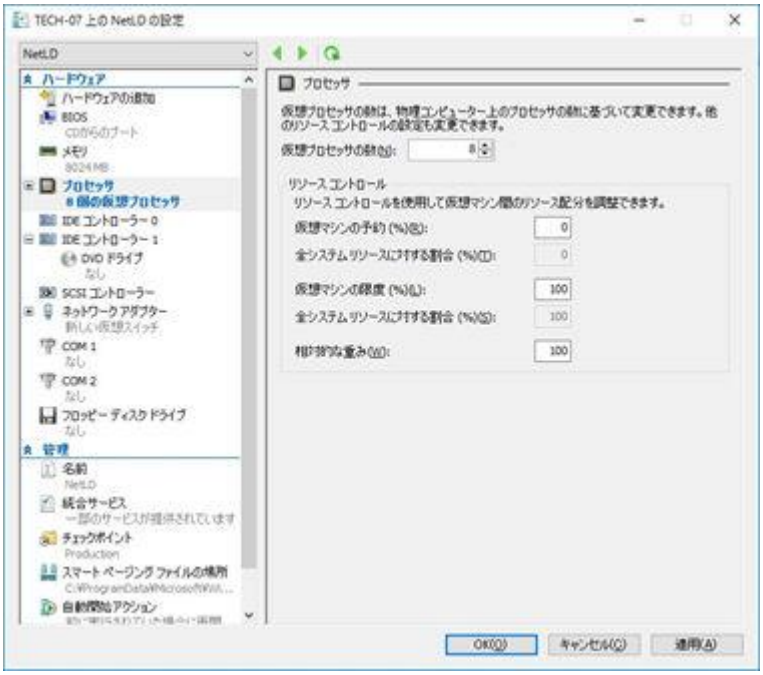
以上で仮想マシンが作成されます。

続いて、2 つの VHDX ファイルを作成した仮想マシンに割り当てます。

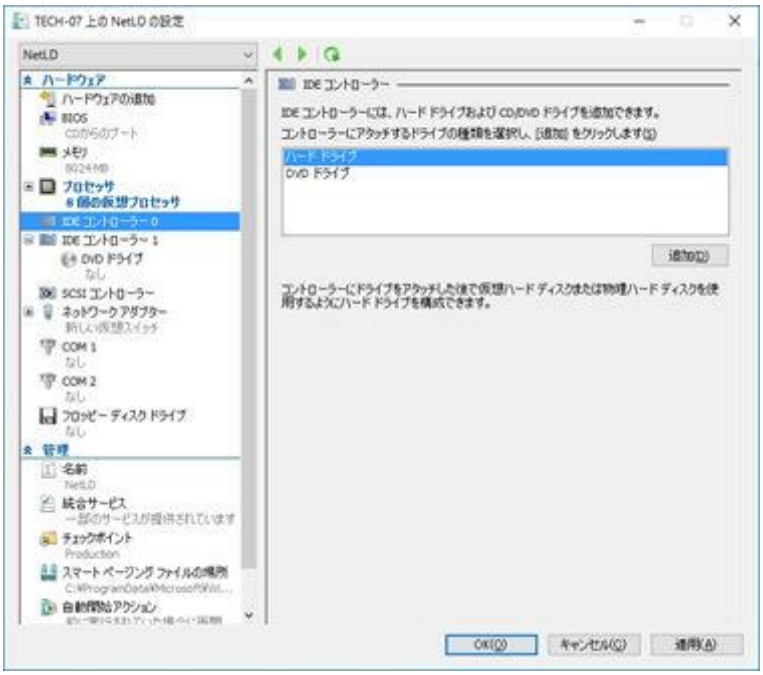
8. 作成した仮想マシンを右クリックし、「設定」をクリックします。



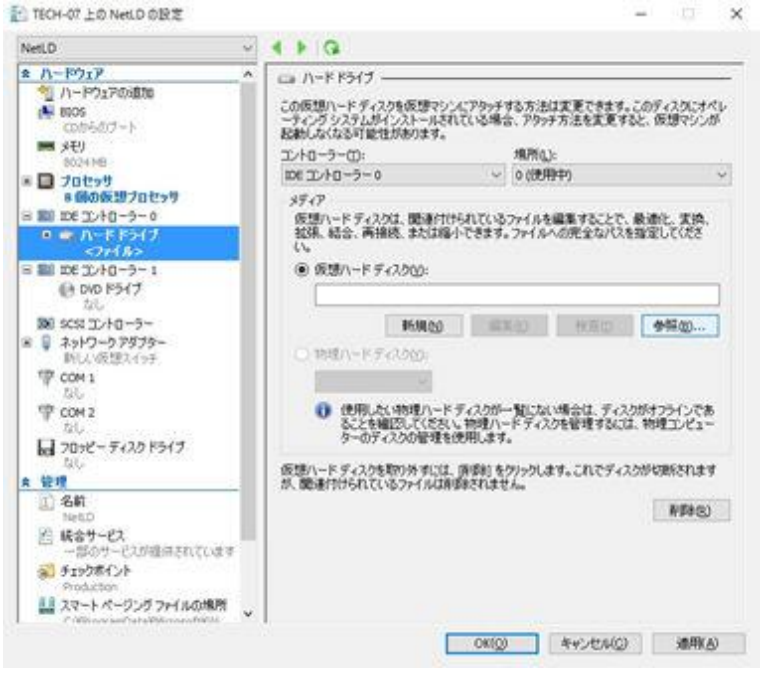
9. 「プロセッサ」を選択し、「仮想プロセッサ数」を変更します。



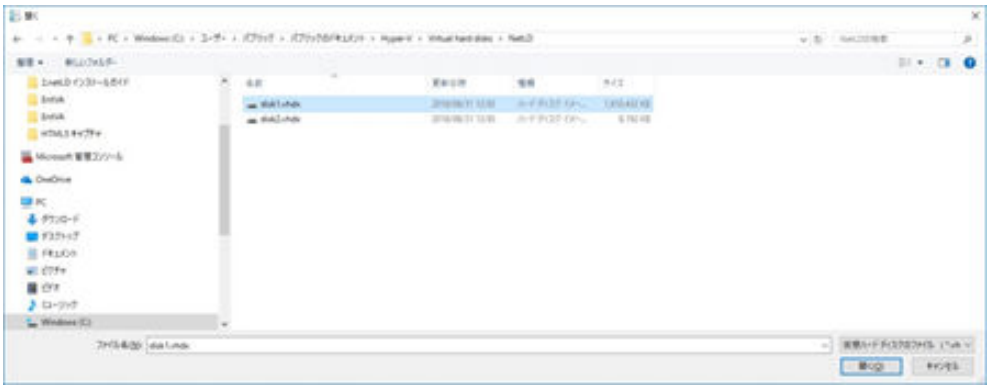
10. 「IDE コントローラー 0」を選択し、「追加」をクリックします。



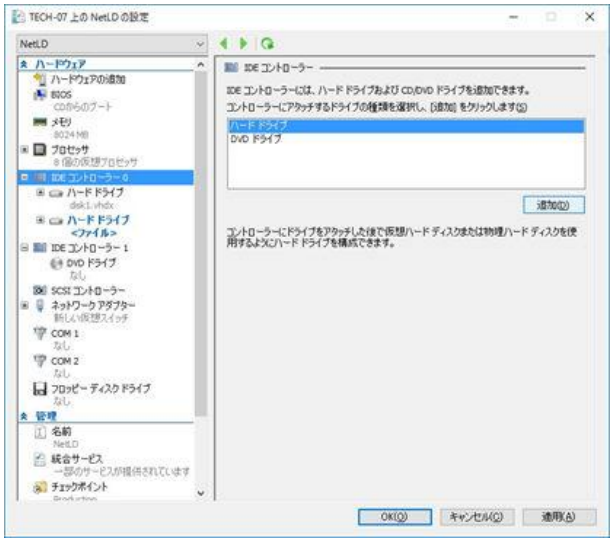
11. 「参照」をクリックします。



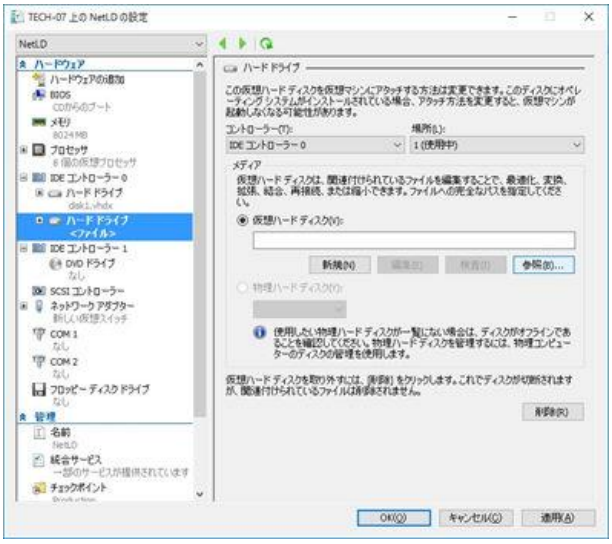
12. 「disk1」を追加し、「OK」をクリックします。



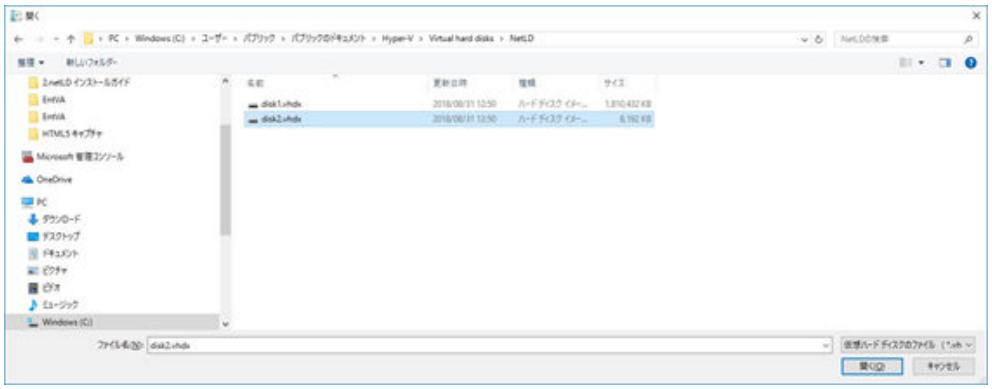
13. 再度、「IDE コントローラー 0」を選択し、「追加」をクリックします。



14. 「参照」をクリックします。

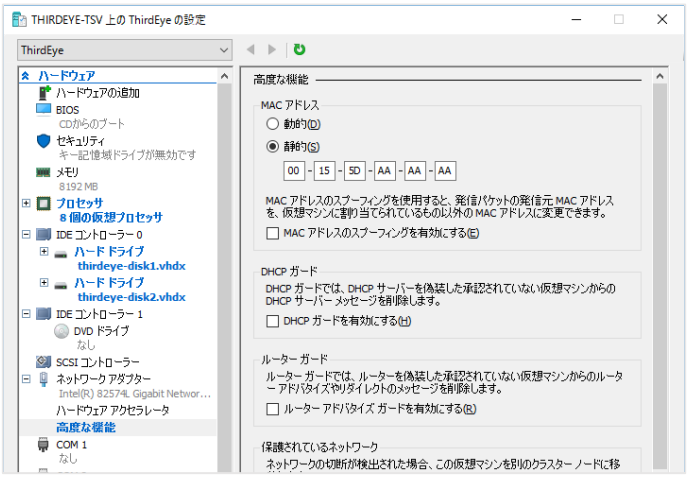


15. 「disk2」を追加し、「OK」をクリックします。



16. ネットワークアダプタ内の「高度な機能」をクリックし、MAC アドレスを「静的」に変更します。

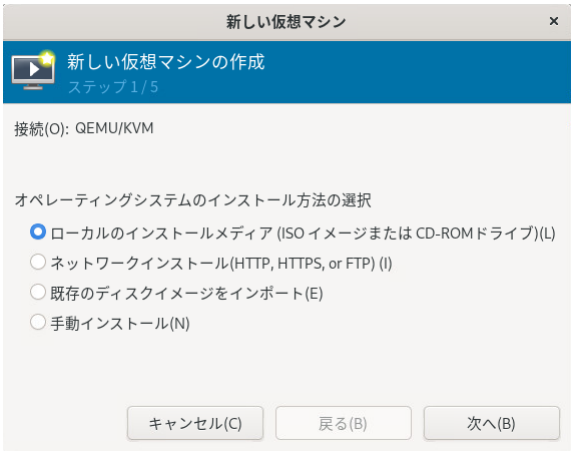
※ 本製品のライセンスは MAC アドレスで管理されています。仮想マシンに割り当てられた MAC アドレスが変更されないように「静的」に設定してください。



2.1.3 Linux KVM へのデプロイ

Linux KVM へのデプロイ手順について説明します。KVM にデプロイする場合は「qcow2」ファイルを使用します。KVM へのデプロイは CLI を使用して行うこともできますが、netLD の IP アドレスなどの設定は GUI から行う必要があります。ここでは、GUI を使用してデプロイする方法について説明します。

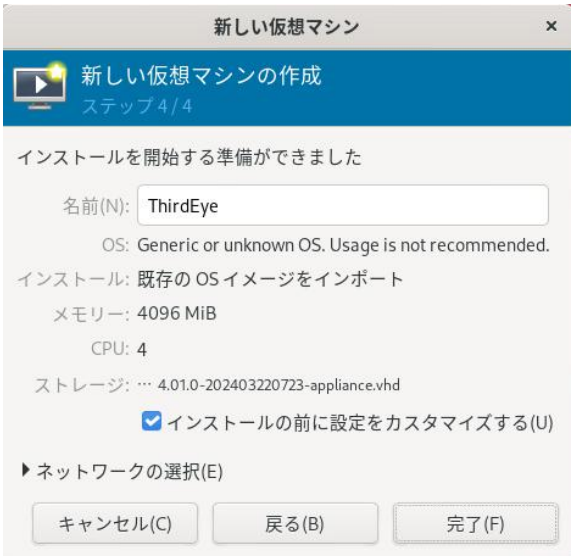
1. 任意のディレクトリに qcow2 ファイルを保存します。（例：/var/lib/libvirt/images）
2. 「仮想マシンマネージャー」を起動します。
3. ファイルメニューから「新しい仮想マシン」をクリックします。
4. 「既存のディスクイメージをインポート」を選択し、「次へ」をクリックします。



5. 「既存のストレージのパスを指定してください」にアップロードしたファイルを指定します。

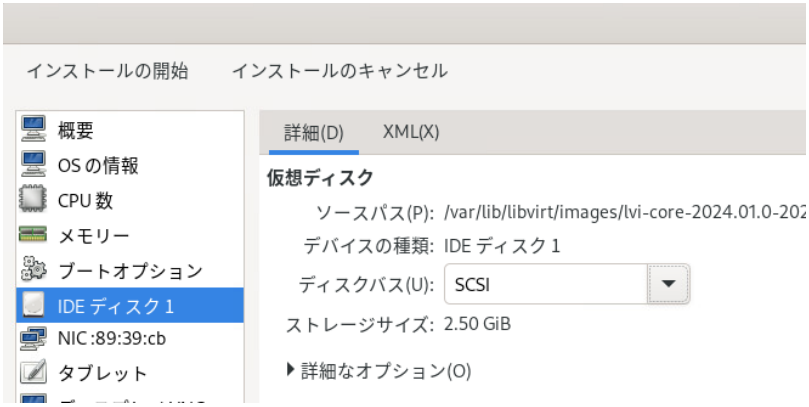
6. 「インストールするオペレーティングシステムの選択」で「Generic or unknown OS」を選択し、「次へ」をクリックします。
7. 割り当てるリソースを入力し、「次へ」をクリックします。

8. 仮想マシンの名前を入力し、「インストールの前に設定をカスタマイズする」にチェック入れます。



9. ネットワークの選択を開き、ネットワーク環境に合わせたデバイスを選択し、「完了」をクリックします。

10. 「IDE ディスク 1」をクリックし、ディスクバスを「SCSI」に変更します。



11. 「ハードウェアの追加」をクリックし、50GB 以上のストレージを追加します。

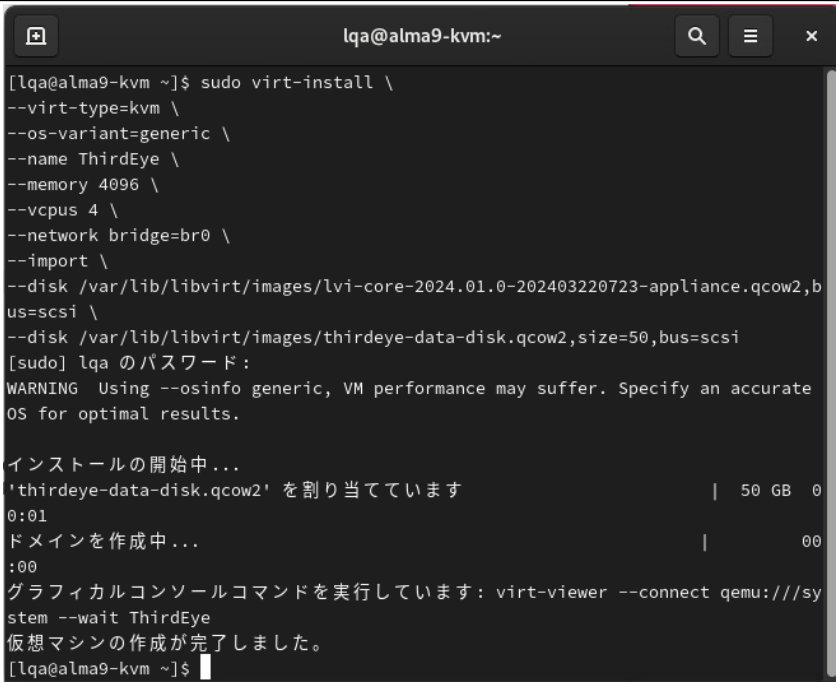
12. 「インストールの開始」をクリックします。

以上で、KVM へのデプロイは完了です。

2.1.3.1 CLI でデプロイする場合のコマンド例

以下は、CLI を使用してデプロイする場合のコマンドの例です。以下のコマンドは、AlmaLinux 9.3 および Virtual Machine Manager4.1.0 を使用しています。バージョンによってオプションの指定方法が異なる可能性があります。

```
sudo virt-install --virt-type=kvm --os-variant=generic ¥
--name ThirdEye --memory 4096 --vcpus 4 --network bridge=br0 ¥
--import ¥
--disk /var/lib/libvirt/images/lvi-core-2024.01.0-202403220723-appliance.qcow2,bus=scsi ¥
--disk /var/lib/libvirt/images/thirdeye-data-disk.qcow2,size=50,bus=scsi
```

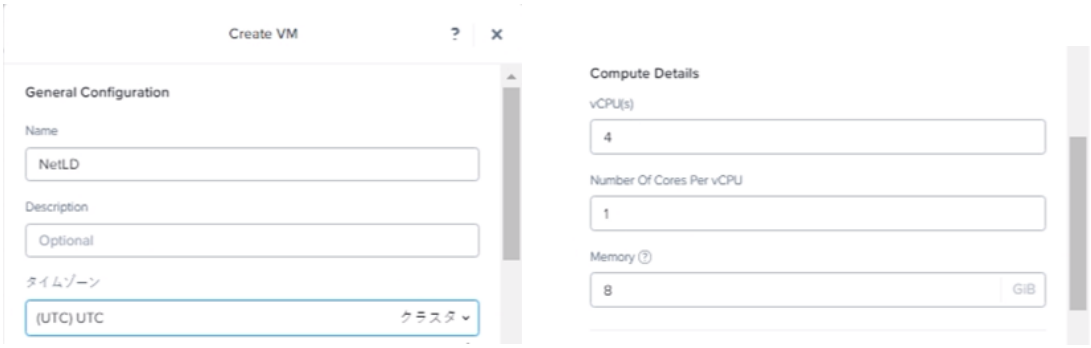


2.1.4 Nutanix AHV へのデプロイ

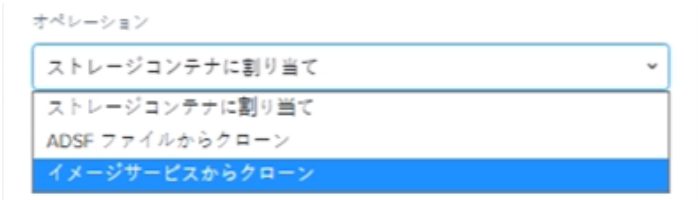
Nutanix AHV へのデプロイ手順について説明します。Nutanix AHV にデプロイする場合は「qcow2」ファイルを使用します。ここではバージョン 6.5.3.6LTS を使用した場合を例に説明します。

1. Nutanix Prism にログインし、画面上部のプルダウンメニューから「設定」に移動します。
2. 左のメニューから「イメージ設定」をクリックします。
3. 「イメージをアップロード」をクリックします。

4. 「Name」と「Storage Container」を入力します。
5. 「Upload a file」に qcow2 ファイルを指定し、「Save」をクリックします。
6. アップロード完了後、画面上部のプルダウンメニューから「仮想マシン」に移動します。
7. 「仮想マシンを作成」をクリックします。
8. 任意の VM 名と割り当てるリソースを入力します。



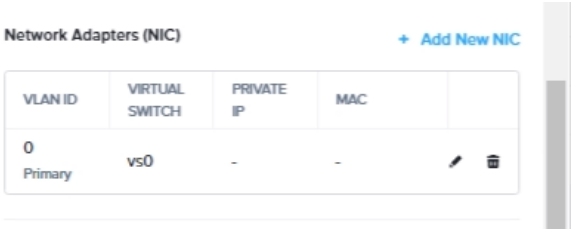
9. 「Add New Disk」をクリックします。
10. Operation プルダウンから「イメージサービスからクローン」を選択します。



11. Image プルダウンから作成したイメージを選択し、追加します。

12. 再度「Add New Disk」をクリックします。
13. サイズを 50GB 以上に設定し、追加します。

14. 「Add New NIC」から、NIC を追加します。

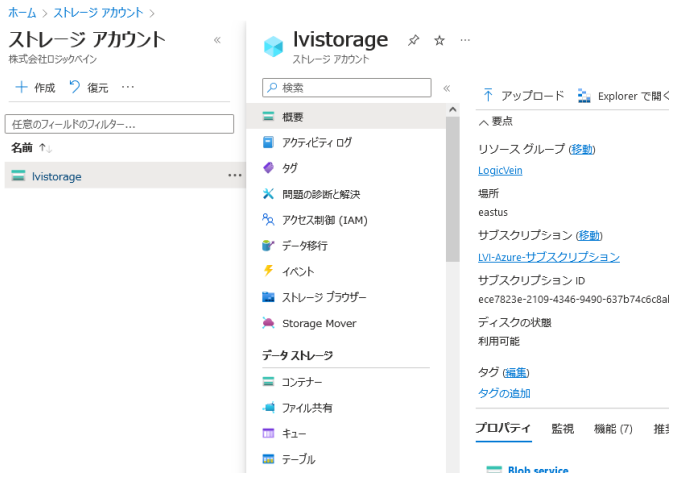


15. 「Save」をクリックします。
16. 仮想マシンが作成されたら、パワーオンします。

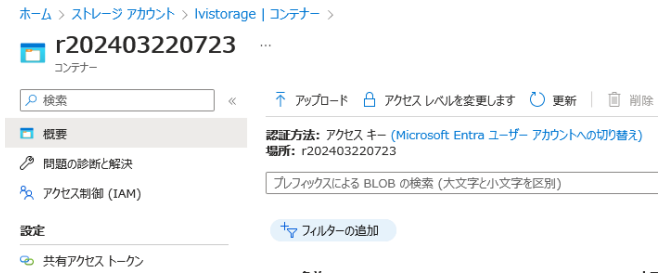
2.1.5 Microsoft Azure へのデプロイ

Microsoft Azure へのデプロイ手順について説明します。Azure にデプロイする場合は、「VHD」ファイルを使用します。

1. Azure にログインし、「ストレージアカウント」サービスに移動します。
2. 既存のストレージアカウントをクリック、または「作成」からストレージアカウントを作成します。
3. ストレージアカウントメニュー内の、「データストレージ」->「コンテナー」をクリックします。

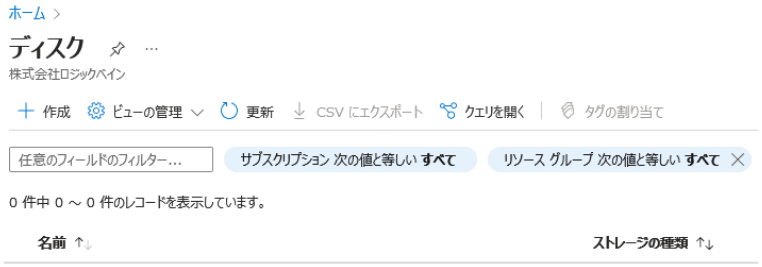


4. 既存のコンテナーをクリック、または「コンテナー」からコンテナーを作成します。
5. 「アップロード」をクリックします。

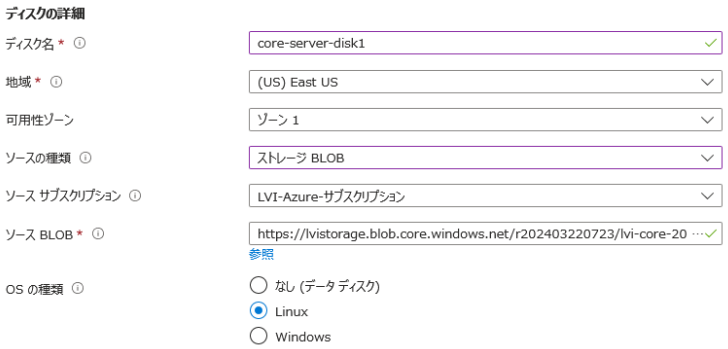


6. ダウンロードした VHD ファイルを選択します。
7. 「詳細設定」を開き、BLOB の種類を「ページ BLOB」に変更します。

8. 「アップロード」をクリックします。
9. アップロード完了後、「ディスク」サービスに移動します。
10. 「作成」をクリックします。



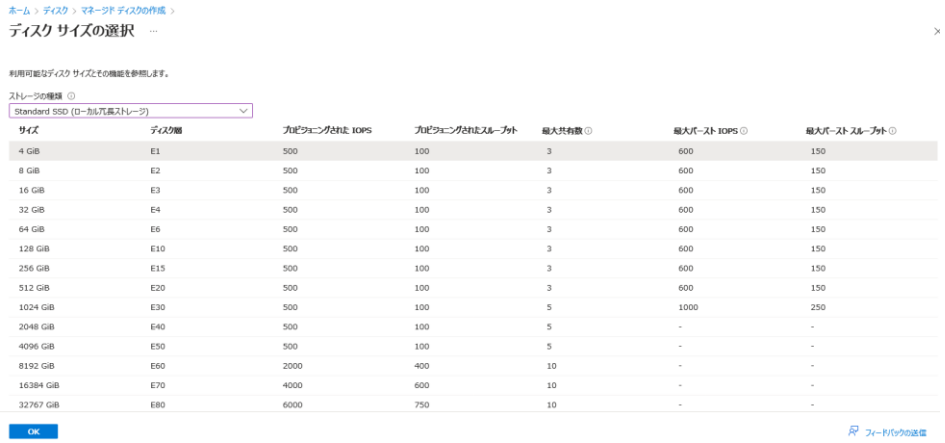
11. サブスクリプション、リソースグループ、地域を選択します。
12. ディスク名を入力します。
13. ソースの種類を「ストレージ BLOB」に変更し、ソース BLOB をアップロードしたファイルを選択します。



14. OS の種類を「Linux」に変更します。
15. サイズ項目で、サイズの変更をクリックします。

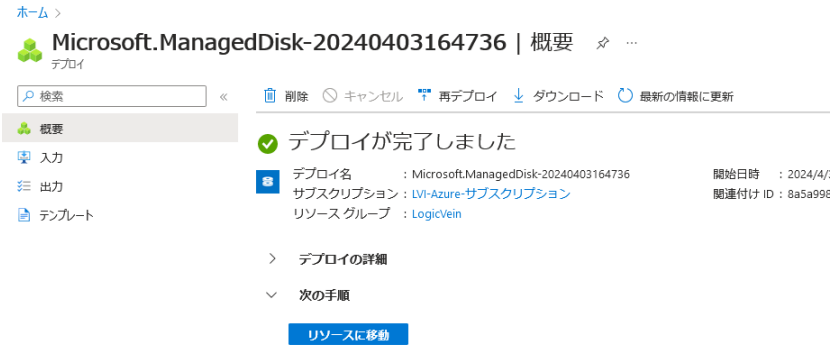
16. 環境にあった「ストレージの種類」を選択します。（SSD を推奨）

17. 一番上の 4GB を選択し、「OK」をクリックします。

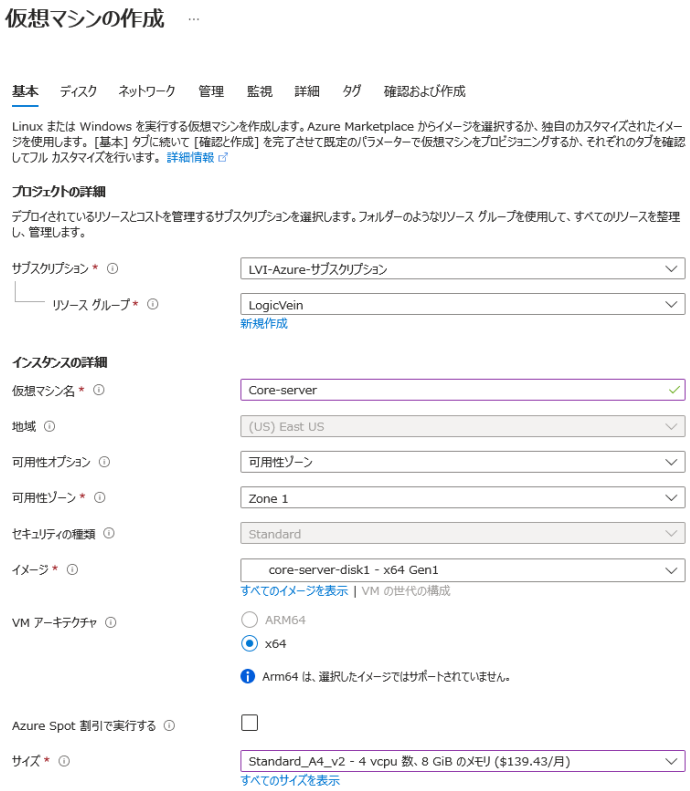


18. 「確認および作成」をクリックします。
19. 内容を確認し、「作成」をクリックします。

20. 作成完了後、「リソースに移動」をクリックします。



21. 「VM の作成」をクリックします。
22. 仮想マシン名を入力します。
23. サイズで仮想マシンに割り当てるリソースを選択します。



24. 「ディスク」タブに移動します。
25. データディスク項目で「新しいディスクを作成し接続する」をクリックします。
26. サイズ項目で、サイズの変更をクリックします。
27. 環境にあった「ストレージの種類」を選択します。（SSD を推奨）

28. 64GB 以上のディスクを選択し、データディスクを追加します。

29. ホストキャッシュが「読み取り/書き込み」になっていることを確認します。

30. 「ネットワーク」タブに移動し、Azure 環境に合わせてネットワークを設定します。

31. 「確認および作成」をクリックします。

32. 内容を確認し、「作成」をクリックします。

以上で、Azure へのデプロイは完了です。

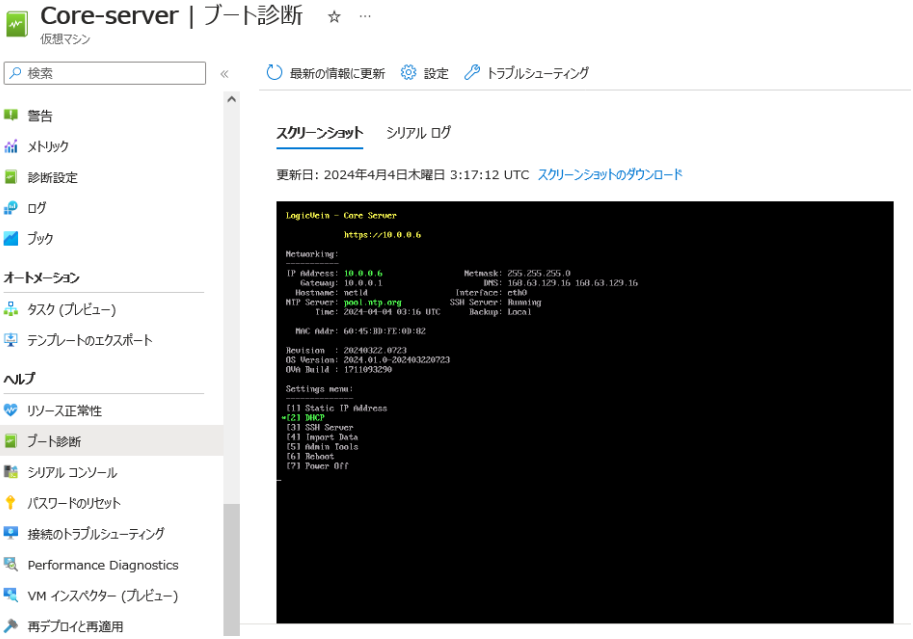
2.1.5.1 受信ポートルールの作成

Azure 上に作成された仮想マシンは、デフォルトで外部からのアクセスが制限されています。そのため、製品画面にアクセスするためのポート（443）や監視/管理に必要なポートなどを別途設定する必要があります。ルールは、ネットワーク設定メニュー内のルールセクションで作成します。

使用するポートについては「エラー! 参照元が見つかりません。 エラー! 参照元が見つかりません。」を参照し、必要なポートを設定してください。

2.1.5.2 MAC アドレスの確認方法

MAC アドレスなどは、［ヘルプ］→［ブート診断］に表示されるスクリーンショットで確認できます。



※既存の netLD 環境を Azure 環境に移行する場合、既存の netLD 環境でシステムバックアップを取得し、Azure 環境へ復元する事を推奨します。

2.1.6 AWS へのデプロイ

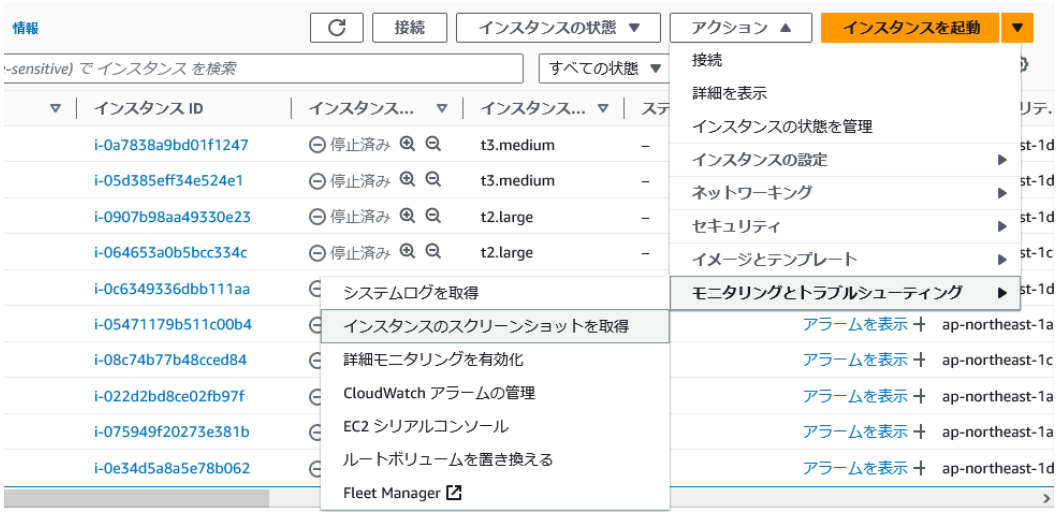
AWS へのデプロイ手順について説明します。AWS にデプロイする場合は、AWS 上のコミュニティ AMI から AMI を選択し、インスタンスを作成します。

1. AWS EC2 にログインし、「インスタンスを起動」をクリックします。
2. 名前を設定し、必要に応じてタグを設定します。
3. アプリケーションおよび OS イメージで、「その他の AMI を閲覧する」をクリックします。
4. コミュニティ AMI を選択し、検索欄に「lvi-core」と入力して検索を実行します。

5. インスタンスタイプで、サイジングガイドラインに従ってタイプを選択します。
   ※ メモリが 4GB 未満の場合、正常に動作しません。システム要件については、以下を参照してください。
   - netLD: https://www.lvi.co.jp/NetLD/
   - ThirdEye: https://www.lvi.co.jp/ThirdEye_system/
6. キーペア（ログイン）でキーペアを作成後、キーペアのダウンロードをクリックします。
7. ネットワーク設定でグループを割り当てます。既存のセキュリティグループを選択するか、新しいセキュリティグループを追加することができます。
   ※ セキュリティ設定については「エラー! 参照元が見つかりません。 エラー! 参照元が見つかりません。」を参照して、必要なポートを設定してください。
8. ストレージを設定で新しいボリュームの追加をクリックし、サイズを 50GB 以上に設定します。
9. 完了したら、「インスタンスを起動」をクリックします。

2.1.6.1 MAC アドレスの確認方法

MAC アドレスなどは、［アクション］→［モニタリングとトラブルシューティング］→［インスタンスのスクリーンショットを取得］から確認できます。



※既存の netLD 環境を AWS 環境に移行する場合、既存の netLD 環境でシステムバックアップを取得し、AWS 環境へ復元する事を推奨します。

2.1.7 Podman へのデプロイ

Podman は、コンテナー化されたアプリケーションのデプロイと管理を目的として設計されたコンテナー化ツールであり、Docker の代替手段として機能します。netLD は Podman コンテナーインフラストラクチャ上にデプロイできます。

2.1.7.1 Podman の機能

- セキュリティ機能: daemon を必要とせず、隔離された環境でコンテナーを実行する事が可能です。
- rootless 機能: root 権限なしでコンテナーの実行をサポートします。（ただし、低ポートバインディングなどの一部の操作には sudo が必要となる場合があります。）
- Docker 互換性: Docker と同様のコマンド構造を使用します。例えば docker run の変わりに podman run を使用します。

例: docker を podman に置き換えた場合:

docker pull harbor.logicvein.com/lvi/lvi-netld-core:2025.07.0-202508260025

2.1.7.2 Podman デプロイ

Podman/Docker ビルドは、LogicVein の Harbor インスタンスに公開されます。バックグラウンドで Docker コンテナ実行するには、オプション「--detach」を追加します。

実行例:

```
Podman run ¥
  --detach ¥
  --name netLD ¥
  --env LICENSE_SERIAL=<SERIALNUM> ¥
  --env JAVA_OPTIONS="-DNAT_RETURN_ADDRESS=<HOST-IPADDR>" ¥
  --ulimit nofile=8192:8192 ¥
  --ulimit nproc=128294:128294 ¥
  --pids-limit=-1 ¥
  --memory=8g ¥
  --cpus=4.0 ¥
  --sysctl net.ipv4.ping_group_range="0 9999" ¥
  --volume <DATA-DIR> ¥
  --publish 20:20 ¥
  --publish 21:21 ¥
  --publish 69:69/udp ¥
  --publish 443:443 ¥
  --publish 2222:2222 ¥
  --publish 50000-50031:50000-50031 ¥
  --cap-add=NET_RAW ¥
  --cap-add=NET_ADMIN ¥
  harbor.logicvein.com/lvi/lvi-netld-core: 2025.07.0-202508260025
```

SELinux が有効なシステム（例：RedHat）では、Docker / Podman を”sudo podman run”で実行できます。これによ

り、このコンテナー専用のディレクトリに対して SELinux コンテキストが設定されます。または、次のコマンドを使用して手動で SELinux コンテキストを設定することもできます。

例：

sudo semanage fcontext -a -t container_file_t "/home/lvi/data2(/.)?"*

sudo restorecon -Rv /home/lvi/data2/

これにより、このディレクトリの SELinux コンテキストが設定され、あらゆるコンテナーがこのフォルダにアクセスできるようになります。

例：

drwxr-xr-x. 2 lvi lvi unconfined_u:object_r:container_file_t:s0 6 Mar 26 19:37 /home/lvi/data2/

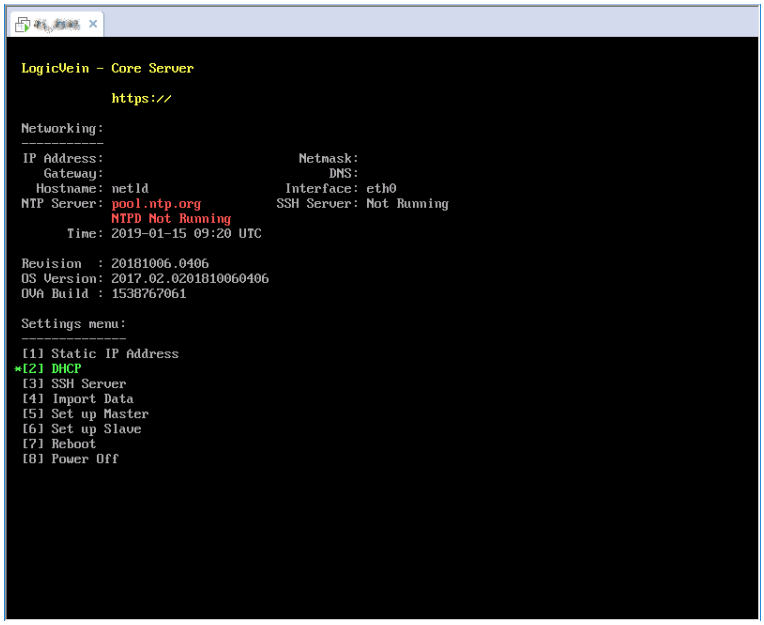
補足	上記のコマンドには、ユーザーが入力する必要がある値が 3 つあります。 ・<SERIALNUM>: ライセンスのシリアル番号で、適用されるシリアル番号と必ず一致させる必要があります。 ・<HOST-IPADDR>: FTP/TFTP のリターンアドレスを指定します。 ・<DATA-DIR>: データが保存されるローカルディレクトリです。通常、OVA 形式のアプライアンスに接続されるデータディスクに相当します。 このディレクトリは存在する必要があります。自動的に作成されません。

2.2 ネットワークを設定する

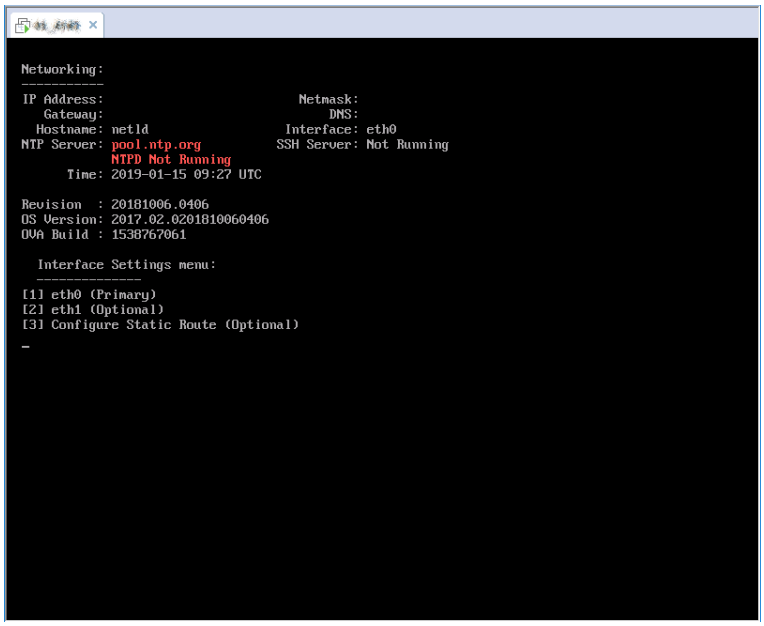
ネットワーク設定では、netLD に割り当てるホスト名や IP アドレスなどを設定します。デフォルトでは、DHCP から IP アドレス等を取得します。DHCP サーバがない環境では、以下の手順で各種設定を行います。

※ ネットワーク設定は、仮想マシンコンソール上でキーボードを使って操作します。

1. キーボードの「1」キーを押し［Static IP Address］を選択します。



2. キーボードの「1」キーを押し［eth0 (Primary)］を選択します。

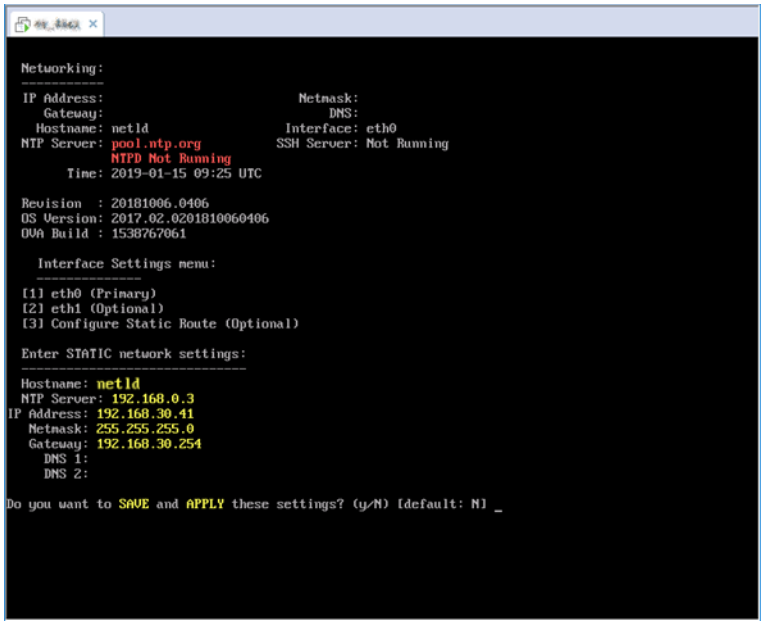


3. 以下のネットワーク設定項目が順に表示されます。キーボードで値を入力し、「Enter」キーを押して次へ進みます。

項目	説明	必須項目
Hostname	仮想アプライアンスで使用するホスト名	必須
NTP Server	仮想アプライアンスで使用する NTP サーバのアドレス（IP アドレスまたはホスト名）	必須
IP Address	仮想アプライアンスで使用する IP アドレス	必須
Netmask	上記 IP アドレスのサブネットマスク	必須
Gateway	ゲートウェイの IP アドレス	必須
DNS 1/2	DNS サーバの IP アドレス	—

注意	仮想マシンコンソールでのキーボード配列は英語配列です。

4. 確認メッセージが表示されます。キーボードの「Y」キーを押して設定を保存します。



設定が完了すると、サービスは自動的に再起動します。

2.3　ライセンスを適用する

ライセンスを適用し、製品をアクティベーションします。

2.3.1　オンライン環境の場合

1. Web ブラウザで、netLD のアドレスを入力してアクセスします。

   https://*<IP_address>*/

   ※　*<IP_address>*には、IP アドレスまたは FQDN（Fully Qualified Domain Name）を指定します。

2. ライセンス認証画面が表示されます。ライセンス番号をコピー&ペーストして入力し、［認証］をクリックします。

サービスが自動的に再起動され、ライセンス適用は完了します。

2.3.2 オフライン環境の場合

1. Web ブラウザで、netLD のアドレスを入力し、アクセスします。

   https://*<IP_address>*/

   ※ *<IP_address>*には、IP アドレスまたは FQDN（Fully Qualified Domain Name）を指定します。

2. ライセンス認証画面が表示されます。アクティベーションキーをコピー&ペーストして入力し、［認証］をクリックします。

サービスが自動的に再起動され、ライセンス適用は完了します。

2.4　初期設定（詳細設定）

ライセンスを適用後、初回アクセス時に［詳細設定］画面が表示されます。この画面では、admin ユーザのパスワードやメールサーバを設定できます。

カテゴリー	項目	必須項目
admin ユーザ設定	admin ユーザのメールアドレス	—
	admin ユーザのログインパスワード	必須
ロケール設定	メール送信時の言語	—
	メール送信時のタイムゾーン	—
サーバ設定	ブラウザタブの表示名	—
	メール等のリンクアドレスに使用するホスト名または IP アドレス	—
メール設定	SMTP サーバのホスト名または IP アドレス	—
	メール送信時のメールアドレス	—
	メール送信時の差出人名	—

注意	パスワードを設定するには、以下の条件を満たしている必要があります。 • 8 文字以上であること • 推測されやすい文字列（人名や固有名詞、辞書に載っている単語、よく使われるパスワード）でないこと • 同じ文字の繰り返しやわかりやすい並びの文字列でないこと

設定後、［保存］をクリックし、ログイン画面に進みます。

3. ログイン／ログアウト

ログイン・ログアウトするには、以下の手順に従ってください。

3.1 ログインする

1. Web ブラウザで、netLD のアドレスを入力してアクセスします。

   https://<IP_address>/

   ※ <IP_address>には、IP アドレスまたは FQDN（Fully Qualified Domain Name）を指定します。

2. ログイン画面で、ユーザ名（admin）・パスワードを入力し、ログインします。

※新規インストールの場合、「2.3.3 初期設定」で admin ユーザのパスワードを設定しています。

ログインすると、netLD のトップ画面が表示されます。

3.2 ログアウトする

1. 画面右上にある［ログアウト］をクリックします。

ログアウトすると、netLD のログイン画面が表示されます。

4. 画面構成

4.1 画面の構成と各部の役割

netLD の画面構成について説明します。

4.1.1 ペイン

ペインとは、ブラウザ画面を上下や左右に分割したものです。以下の画面は、通常 netLD をブラウザで表示した場合の画面の例です。

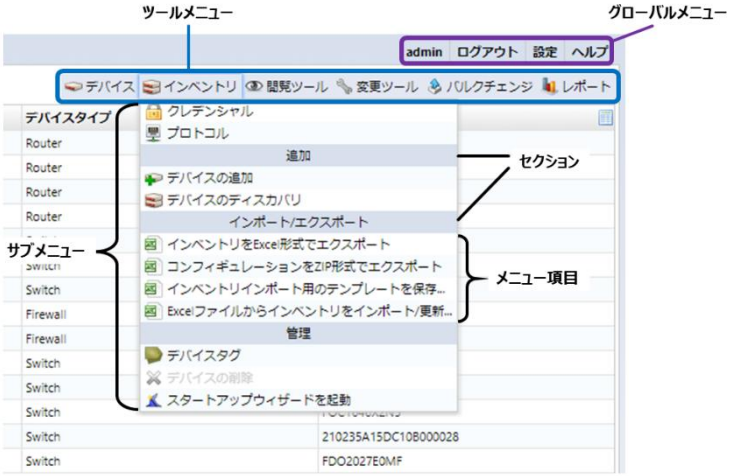
netLD を使う上でもっとも重要なペインは上半分の*メインペイン*と、下半分の*ステータスペイン*です。これらのペインは、 画面中央の小さな三角ボタン（切替えボタン）を押すことによって、メインペインだけ、あるいはステータスペインだけを表示するように切り替えることができます。どちらのペインも、複数の*タブ*をもっています。

メインペインとステータスペインとは完全に独立して動いています。下のペインを変えないまま上のペインのタブを切り替えたり、上のペインを変えないまま下のペインのタブを切り替えたりすることができます。

この性質のため、複数の操作を上と下で同時に行うことが可能になります。例えば、メインペインから登録タブをステータスペインに開き、続いてメインペインをデバイスタブに切り替え、デバイスタブから下の登録タブにデバイスを登録する、などです。この操作は*タブ切り替えテクニック*として一部の操作（ジョブの作成など）で必要になります。

4.1.2 メニューとサブメニュー

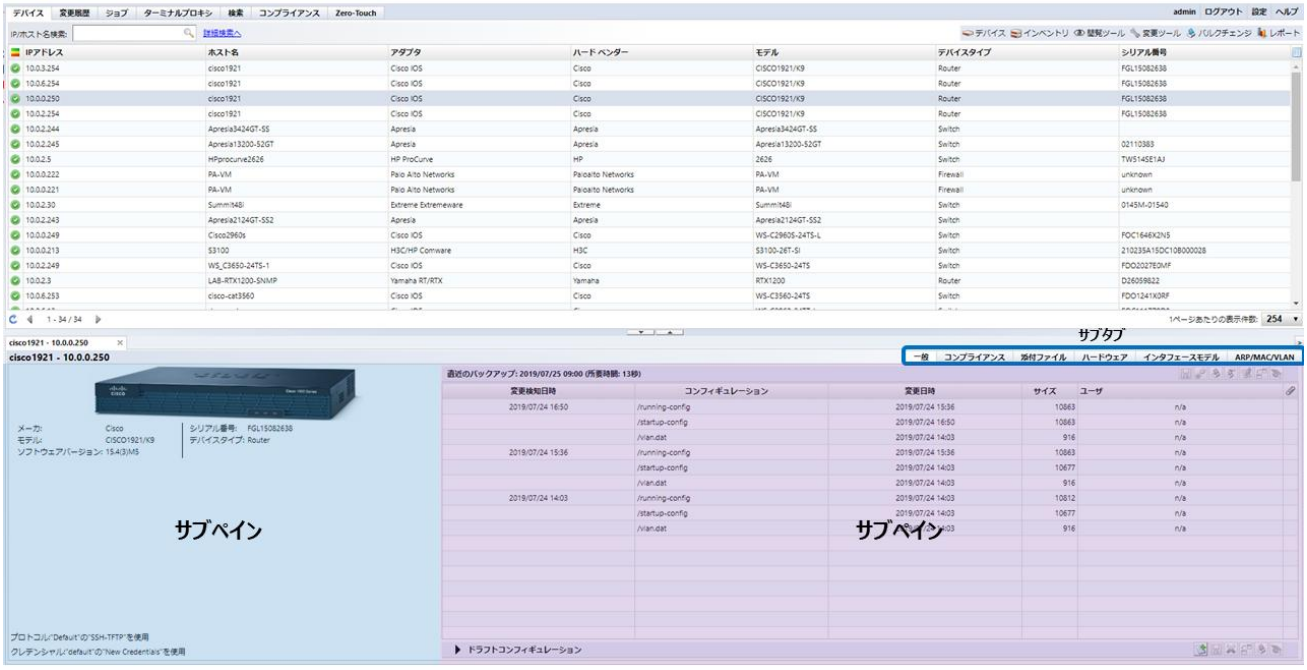
以下の画面はグローバルメニューとツールメニューに分かれています。ツールメニューはデバイスタブのメニューで、図では青色の枠で表示してあります。一方グローバルメニューは紫色の枠で表示されています。グローバルメニューは、「サーバ設定ウィンドウ」にアクセスできる点が重要です。「サーバ設定ウィンドウ」は、単純に「設定ウィンドウ」と呼ばれることもあります。



ツールメニューの各要素を押すと、*サブメニュー*が現れます。*サブメニュー*はいくつか*セクション*に別れています。セクションの中に複数のメニュー項目があります。

4.1.3 サブタブとサブペイン

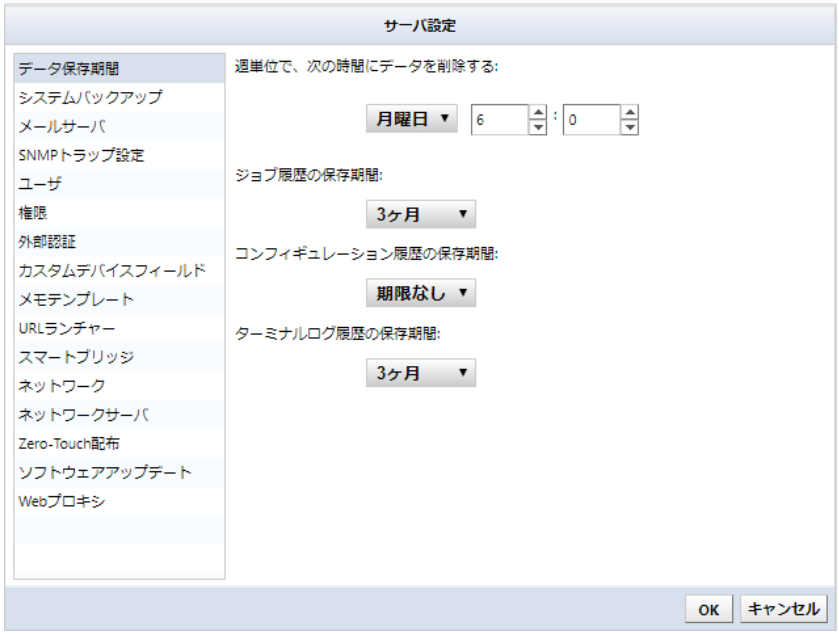
ステータスペインは左右にわかれており、これはサブペインと呼びます。それぞれのサブペインがタブを持つ場合、これを*サブタブ*と呼びます。



4.1.4　サーバ設定

グローバルメニューの[設定]をクリックすると、「サーバ設定ウィンドウ」が開かれます。

左のサブペインに沢山のメニューがあり、それぞれのメニューを選ぶと右のサブペインで設定を行うことができます。OK ボタンを押すと、行った設定変更がすべて適用・保存されます。キャンセルボタンを押すと、行った設定変更は破棄されます。小さなウィンドウはダイアログとも呼びます。最もよく現れるウィンドウはサーバ設定ウィンドウです。サーバ設定ウィンドウは、単純に「設定ウィンドウ」と呼ばれることもあります。このウィンドウには、netLD のすべての設定が集約されています。netLD の動作を変更する際には、必ずと言って良いほどこのウィンドウを開くことになるでしょう。



5. 基本操作

この章では、マニュアルの全体で用いられることになる用語について解説します。用語には、基本的な画面のパーツから、デバイスの分類に用いる概念など、様々なレベルのものがあります。どの用語も一般のコンピュータやネットワークの知識から類推できる範囲の言葉です。

5.1 バックアップ

デバイス設定を変更するためのインタフェースについて解説します。デバイスビューの行はそれぞれのデバイスに対応しており、行をダブルクリックすると ステータスペインがデバイスのプロパティとバックアップ履歴を表示します。

5.1.1 バックアップステータス

ステータスアイコンはデバイスのバックアップの状態に伴って変化します。アイコンは、コンプライアンス違反が検知された場合にも変化します。上図では、青枠で囲われた部分がバックアップステータスです。

5.1.2 デバイスビュー

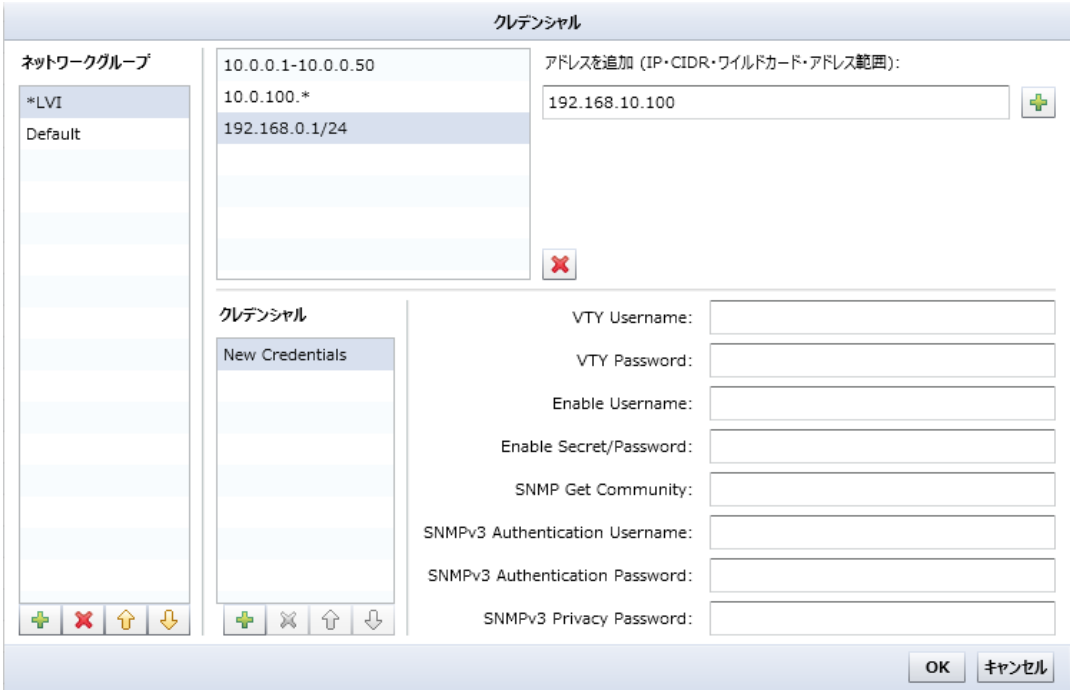
インベントリ内のすべてのデバイスを表示します。上で述べたように、列をダブルクリックすればデバイスのコンフィギュレーションを閲覧することができます。 図では水色に示されています。

この画面に表示される情報はデバイスごとに変わります。特定の情報を持っていない デバイスでは、表示されない欄があります。

デバイスビューでは、デバイスをクリックによって選択できますが、よくあるファイルマネージャと同様、シフトキーやコントロールキーを押したままクリックすることで複数のデバイスを選択することもできます。シフトキーを押せば、前回押したところから今回押したところまでの範囲にあるデバイス全てを選択できます。コントロールキーを押すと、選択にひとつひとつ要素を 追加できます。

5.2 クレデンシャル

クレデンシャルは、デバイスごとのログイン及びセキュリティ情報をまとめるためのものです。この情報を netLD に与えることで、netLD はデバイスの情報にアクセスできるようになります。クレデンシャル情報はクレデンシャルウィンドウから追加することができ、このウィンドウは[インベントリ] → [クレデンシャル]から開くことができます。



クレデンシャルウィンドウでは、デバイスにアクセスするのに必要なすべての情報（ユーザ名、パスワード、SNMP コミュニティストリングなど）を登録してください。ログインに必要のないものは登録しませんが、必要なもののうちに一つでも足りない要素があると、netLD は基本的などの操作も実行することができません。（バックアップなど）それぞれのクレデンシャルは、以下のような要素を持ちます。

クレデンシャル項目の説明:

項目	説明
VTY Username/VTY Password	ネットワーク機器に CUI 経由でログインする際に必要なユーザ名/パスワードです。CUI 経由とは、ssh や telnet、rlogin などのリモート端末を指します。
Enable Username	管理者のユーザ名です。デバイス上では、このユーザだけがコンフィギュレーションを変更することができます。
Enable Secret/Password	CISCO デバイスで使用可能な 2 つのパスワードの一つです。イネーブルシークレットパスワードのほうが、単なるイネーブルパスワードよりもセキュリティ上堅牢です。シークレットパスワードを使えるデバイスでは、可能な限りこれを用いてください。
SNMP Get Community	SNMP での Get Community 要素を指定します。
SNMPv3 Authentication Username	SNMPv3 で定義された、認証ユーザ名を入力してください。
SNMPv3 Authentication Password	SNMPv3 で定義された、コミュニティに対するパスワードです。
SNMPv3 Privacy Password	SNMP による通信の際、暗号化に用いられるパスワードです。
SSH Private Key	ネットワーク機器にログインするための SSH 秘密鍵です。

5.3 ネットワークグループ

クレデンシャルを複数まとめてネットワークグループを作ることができます。クレデンシャル情報のネットワークグループは、IP アドレス範囲のリストと、クレデンシャルのリストから成り立ちます。netLD は、あるデバイスへのログインの際、IP を見ることでデバイスがどのネットワークグループに該当するか検索し、また該当するネットワークグループに対して、クレデンシャルのリストを上から順に用いてログインを試みます。

異なるネットワークグループの IP アドレス範囲は重なってはいけません。もし重なると、正しくないクレデンシャルがデバイスに適用される可能性があり、その場合、バックアップやログインに失敗します。

5.4 プロトコル

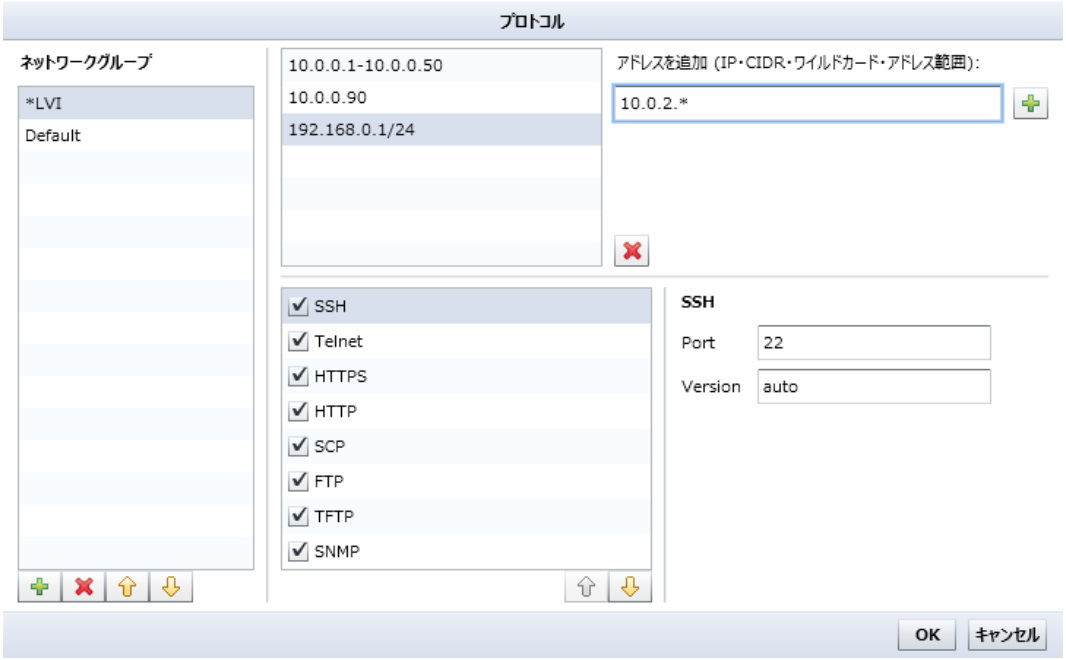
プロトコルは、デバイスに接続するための方法を指定します。これはクレデンシャルと同じく、netLD がデバイスに接続を試みる際に重要な要素になります。プロトコルはインベントリ→プロトコルから変更することができます。

プロトコルウィンドウでは、クレデンシャルと同じく IP 範囲を用いてネットワークグループを定義することができます。 プロトコルのネットワークグループとクレデンシャルのネットワークグループには、名前による対応などの関連性は特にありません。

一つのネットワークグループ内では、指定された IP 範囲に対してどのプロトコルを用いるかを指定することができます。クレデンシャルではログイン情報を指定しましたが、ここではどの種類の通信にどのプロトコルを用いるかの設定を行う点が異なります。

netLD の初期設定では、ただひとつのネットワークグループ Default がはじめから作られています。入力のためのイン

タフェースは、クレデンシャル情報の入力エリアとほぼ同様の形で作られています。



それぞれの入力エリアでは、ある通信プロトコルの仕様を許可する場合には、チェックボックスをオンにします。Default ネットワークグループでは、すべてのプロトコルがデフォルトでチェックされています。

上下ボタンは、どの通信プロトコルを使うかの優先度を指定することができます。netLD は通常最も高い優先度を持つプロトコルを用いてデバイスに接続しようとし、失敗したら次のプロトコルで接続を試みます。

新たなネットワークグループを追加したい場合、ボタンを押してください。

現れるウィンドウにグループ名を入力し、またクレデンシャルと同様に、IP アドレス範囲のアドレスを追加（IP, CIDR, ワイルドカード, アドレス範囲)フィールドに記述してください。最後に右の ボタンを押せば、指定したアドレス範囲が現在開いているプロトコルの中に追加されます。

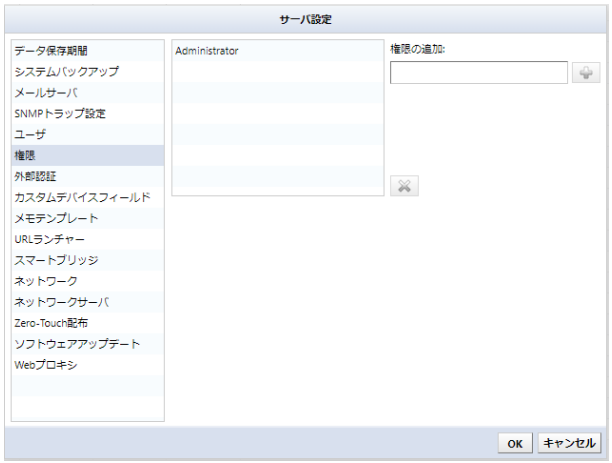
5.5 ユーザと権限

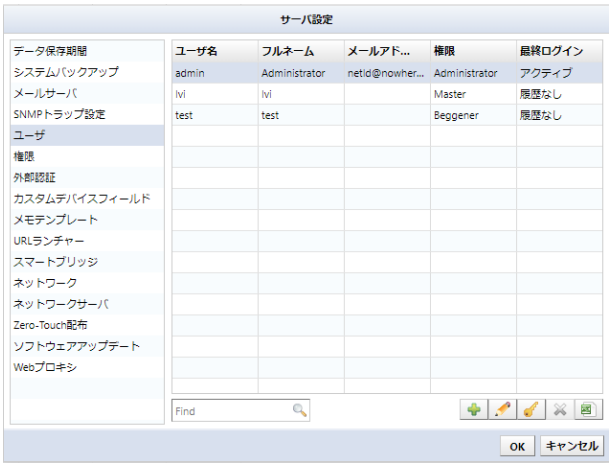
権限はユーザの実行できる操作の範囲を指定します。それぞれの権限は、個別の操作に関する権限を集めたものです。個別の操作の例としては、例えば、デバイスの読み書き操作などです。それぞれのユーザはそれぞれ異なる権限を持つことになります。これらの権限を適切に指定することで、ネットワークに誰がどのように変更を加え、閲覧を行うことができるかを細かく指定することができます。

ユーザ	経験	許可されている操作
	15 年目のベテラン	すべての機能
	5 年目	ネットワーク A、B でのバックアップ、スケジュール、変更

	2 年目	バックアップ、ネットワーク A でのスケジュール、実行
	0 年の新人	バックアップのみ実行

ユーザと権限の設定はサーバ設定ウィンドウから行うことができます。





インストール直後の初期設定では、存在する権限は Administrator のみであり、また存在するユーザは admin という名前のユーザのみです。このユーザのパスワードは password になっています。よりよいセキュリティを目指すならば、このパスワードはインストール後すぐさま十分な長さのパスワードに変更すべきです。また、もし複数のオペレータがデバイスを管理することになった場合には、適切な権限を分割して与えたほうがより好ましくなります。

5.6 ネットワーク

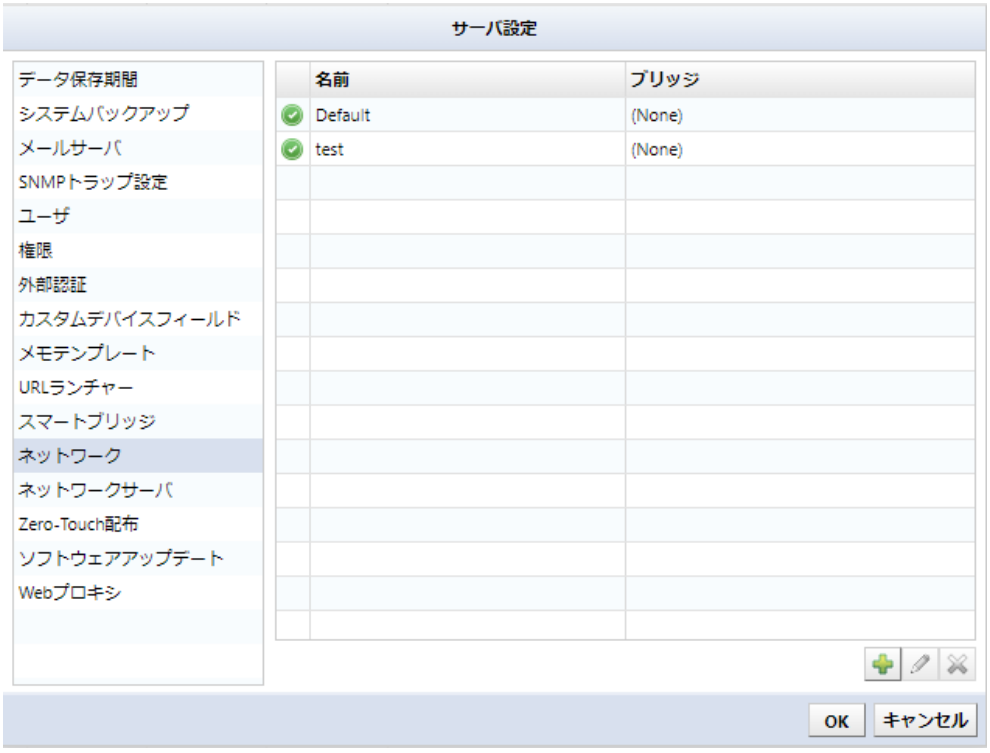
netLD のネットワークは、巨大なインベントリを分割して管理するための概念です。ネットワークセグメントごとにそれぞれのインベントリ、クレデンシャル、プロトコルがあります。権限を与えられている限り、ユーザはネットワークを作成し、またそのインベントリを表示することができます。これは、クレデンシャルやプロトコルの解説で出てきた*ネットワークグループ*とは異なります。(一つの*ネットワークグループ*は、クレデンシャルと IP の集合、あるいはプロトコルと IP の集合です。)

ネットワークは、スマートブリッジとジャンプホストの機能と深く連携します。

スマートブリッジは、独立した IP 空間を持つ複数の LAN をネットワーク越しに管理します。複数の LAN とは、例えば、同じビルの三階と四階にそれぞれの LAN があるような場合です。このとき、三階にある機器 A と四階にある機器 B が同じ IP を持っている可能性があります。この場合、ひとつのインベントリに 2 つの機器 A,B を同時に含めてしまうと、インベントリ内に同じ IP を持つ機器が 2 つ存在することになってしまい、IP アドレスで機器を指定できなくなります。これを回避するために、スマートブリッジは複数の LAN をそれぞれ別のネットワークとして管理します。

※スマートブリッジの詳細は、7.3 スマートブリッジ（オプション）を参照してください。

※ジャンプホストの詳細は、7.4 ジャンプホストを参照してください。



5.7　サービス管理

netLD のアーキテクチャは、サーバクライアント方式を採用しています。サーバプログラムは通常目には見えないバックグラウンドで実行されています。一方、実際にマウスやキーボードの操作できるのは、ブラウザから表示するクライアント GUI プログラムです。GUI は、マウスなどによる操作の内容をサーバに伝えます。GUI を用いてサーバにアクセスするためには、まずサーバが動いていなくてはいけません。したがって、netLD を使うためにはまず初めにサーバを起動する必要があります。また、以下の場合には
netLD は再起動されます。

- netLD サーバの IP アドレスが手動で変更された場合。
- 新たなデバイスアダプタ(対応デバイスを増やすためのプログラムモジュール)が追加された場合。
- バックアップされたファイルが netLD の外で手作業により復元された場合。
- ライセンスファイルが手動で上書きされた場合。
- netLD 自体のバージョンが更新された場合。

6. 基本ツール

この章では、スクリーンショットを交えて netLD の基本ツールの使用方法を解説します。また、一つのツールがメイン機能の大きな部分を占める場合には、単純な使用方法の解説にとどまらず、そのツールの概説と存在理由も説明します。ただし、すでに netLD の基本操作で解説したコンセプトについては、参考リンクを設けています。

6.1 クレデンシャル

ここでは、スタートアップウィザードで解説したクレデンシャルについて、追加、削除、大量追加など詳しい設定方法を見ていきます。

クレデンシャル情報の数がそこまで多くない場合には、複数のネットワークグループを使う必要はありません。すべてのデバイスの IP を含むネットワークグループをひとつ設け、その中にすべてのクレデンシャルを登録すれば、十分に運用を行うことができます。しかし、デバイスとクレデンシャルの数が増えてくると、クレデンシャルをひとつのネットワークグループで管理することは難しくなります。そういった場合には、複数のネットワークグループを設けるのがよいでしょう。

netLD は 2 つのクレデンシャル登録方法をもっています。一つはダイナミック設定、もうひとつはスタティック設定です。ダイナミック設定では、ひとつのネットワークグループが IP の範囲に対応し、そこに該当する全デバイスに対してクレデンシャルを適用します。一方、スタティック設定では個別の IP ごと、つまり個別のデバイスごとにクレデンシャル情報を登録します。スタティック設定では、デバイス情報を手で入力することもできますが、もしも表にまとめられたデータがある場合には、これをエクセルファイルの形で読み込ませることができます。エクセル表からの入力を便利にするために、エクセルファイルのテンプレートを出力する方法も設けています。

6.1.1 ダイナミック設定

では、ダイナミック設定を用いたネットワークグループの追加方法を、スクリーンショットを用いて見て行きます。ツールメニュー-->インベントリ-->クレデンシャルを開いてください。

ウィンドウの左下の  ボタンを押すか、画面中央のボタンを押してください。(この中央のボタンは、クレデンシャルがひとつも登録されていない初期状態でのみ表示されます。)

すると、図のようなダイアログが現れます。新しく作るネットワークグループの名前を入力し、ダイナミックを選択し「OK」ボタンを押してください。これでひとつのネットワークグループが追加されます。

ネットワークグループを作成したら、次に必要な情報を入力します。まず、新規作成したグループの適用範囲を設定します。以下の形式で IP アドレス範囲を入力し追加してください。全てに適用したい場合には、アドレス追加欄に「0.0.0.0/0」を入力します。登録されたアドレスは左の枠内に表示されます。

■IP 範囲の記入例

- 個別 IP アドレス

  10.0.0.1　2001:0DB8:AC10::

- IP アドレス範囲

  192.168.0*　10.0.0.1-10.0.0.100　192.168.0.1/24　2001:0DB8:AC10::/64

IP 範囲を登録したら、次にクレデンシャル情報を登録します。一つのネットワークグループに複数のクレデンシャルを登録する場合には、クレデンシャルと書かれたフィールドの下にある  ボタンを押し、現れるダイアログに新しいクレデンシャルの名前を入力します。

6.1.2 スタティック設定

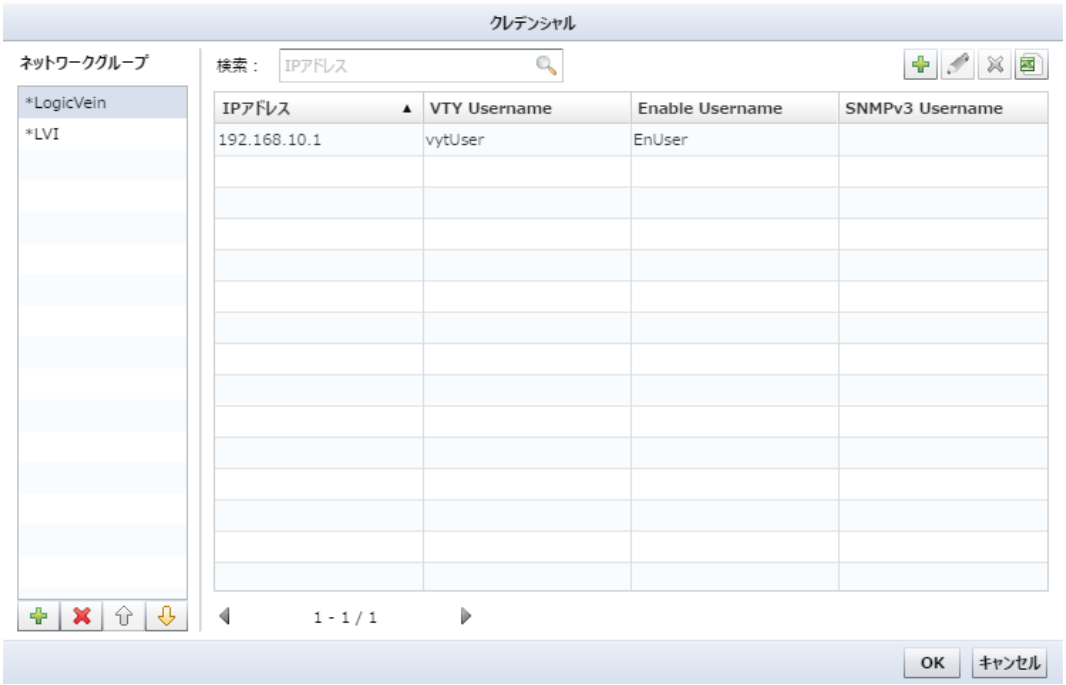
次に、スタティック設定の使用方法を見て行きましょう。ツールメニュー-->インベントリ-->クレデンシャルを開いてください。

ウィンドウ左下の  ボタンを押してください。すると、図のようなダイアログが現れます。新しく作るネットワークグループの名前を入力し、スタティックを選択し「OK」ボタンを押してください。これでひとつのネットワークグループが追加されます。

スタティック設定では、ユーザは完全に手動で IP ごとにクレデンシャルを入力する必要があります。右上の  を押すと、デバイスのクレデンシャルを追加できます。

デバイスのクレデンシャル情報を入力し、OK ボタンを押してください。これで、デバイス 1 つ分の設定が行われました。

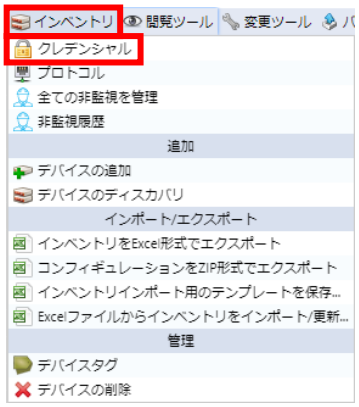
設定をする必要があるすべてのデバイスについて、この作業を行なってください。終わったら、OK を押して終了します。



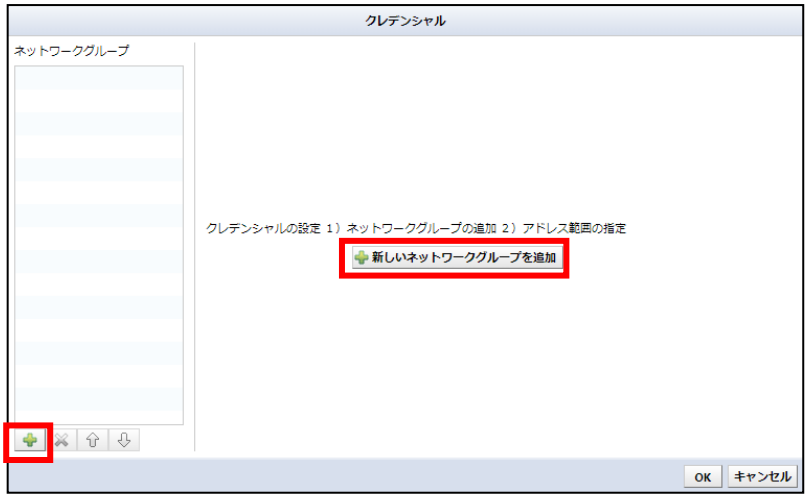
6.1.3 クラウドアカウントのクレデンシャル情報を設定する

リビジョン r20250627.0503 より、netLD はクラウドデバイス管理に対応しました。ここではクレデンシャル設定について説明します。

1. ［デバイス］タブを選択し、［インベントリ］→［クレデンシャル］の順にクリックします。



2. ［＋(追加)］または［新しいネットワークグループを追加］をクリックします。



3. ネットワークグループ名を入力し、［クラウド］を選択して［OK］をクリックします。

4. 作成されたクレデンシャルがネットワークグループに表示されます。

6.1.3.1 クラウドクレデンシャル設定

クラウドデバイスは主にクラウドアカウントを使用してデバイスにアクセスします。クレデンシャル/API アクセストークンがクラウドアカウントにアクセスできるように、以下の項目を設定する必要があります。表示される項目はクラウドサービスによって異なります。他のクレデンシャルとは異なり、アドレスを設定する必要はありません。アドレスフィルタを設定しない事で、ディスカバリ可能な全てのクラウドデバイスを検出します。

(1) Cisco Meraki

クラウドデバイスは主にクラウドアカウントを使用してデバイスにアクセスするため、既存のダイナミックおよびスタ

ティッククレデンシャルに加え、新しいクラウドクレデンシャルタイプを追加しました。Cisco Meraki ではクレデンシャル/アクセストークンがクラウドアカウントにアクセスできるよう、以下の項目を設定する必要があります。

項目	必須項目	説明
クレデンシャル表示名	必須	表示される名前を設定します。
クラウドサービス	必須	クラウドサービスプロバイダを設定します。
API キー	必須	パスワードもしくはアクセストークンを設定します。
アドレスフィルタ	—	IP もしくは CIDR を設定します。

(2) Aruba EdgeConnect

netLD は、HPE Aruba EdgeConnect（EC）デバイス（旧称 SilverPeak）向けのクラウドデバイスサポートを提供します。EdgeConnect デバイスは、導入済みの Orchestrator または Aruba Central クラウドポータルを介してローカルで管理できます。EdgeConnect デバイスでは、Orchestrator またはクラウド ポータルにアクセスするために、API キーと API URL を設定する必要があります。

項目	必須項目	説明
クレデンシャル表示名	必須	表示される名前を設定します。
クラウドサービス	必須	クラウドサービスプロバイダを設定します。
API Base URL	必須	API プロバイダ URL を設定します。
API キー	必須	パスワードもしくはアクセストークンを設定します。
アドレスフィルタ	—	IP もしくは CIDR を設定します。

API URL を設定する際は、IP（ドメイン）とプロキシマッピング（ある場合）のみ設定してください。
netLD が API のベース URL を生成します。URL に https://10.0.99.8/を設定すると、システムは Base URL https://10.0.99.8/gms/rest を生成します。

(3) Aruba Central

netLD は、Aruba Central 経由で Aruba アクセスポイント（AP）をクラウドデバイスとして管理するサポートを提供します。開始前に、API アクセスに必要な権限を持つ有効な Aruba Central アカウントが存在することを確認してください。Aruba アクセスポイントを監視するには、Aruba Central 用のクラウドアカウントクレデンシャル情報を設定し、その情報をディスカバリしてアクセスポイントを検索する必要があります。

Aruba Central 用のクラウドアカウントクレデンシャル情報を設定する際は、まず Aruba Central ポータルからアクセストークンを生成してください。アクセストークンの詳細が利用可能になったら、認証情報ページに移動し、新しいクラウドアカウント認証情報を作成します。Aruba Central API プロバイダはアクセストークンと更新トークンの両方に有効期限を設けています。そのため、ThirdEye はトークンを定期的に更新します。クレデンシャル情報の初期設定時からこの処理が開始されます。クレデンシャルを設定する際は、Aruba Central ポータルで生成したアクセストークンの情報を使用してください。クレデンシャルが設定されると、ThirdEye はアクセストークンの詳細を取得するために初期トーク

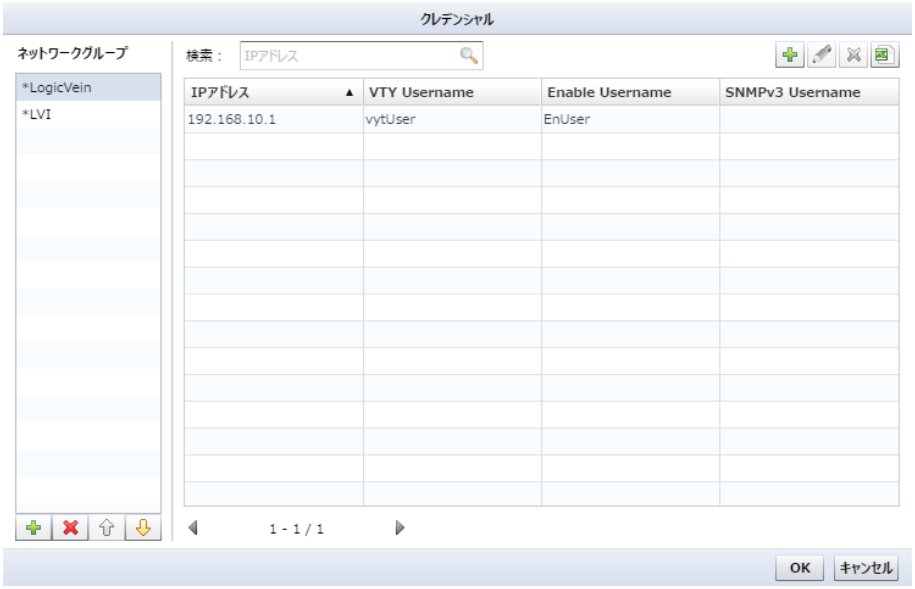
ン更新を実行します。その後、トークンの有効期限の 90%が経過した時点で、トークンは定期的に更新されます。

項目	必須項目	説明
クレデンシャル表示名	必須	表示される名前を設定します。
クラウドサービス	必須	クラウドサービスプロバイダを設定します。
API Region	必須	API Gateway のリージョンを設定します。(アカウントが登録されている地理的クラスタに基づく)。
Client ID	必須	新規で Refresh Token を要求する為の Client ID を設定します。
Client Secret	必須	Refresh Token の為の Client Secret を設定します。
Refresh Token	必須	Refresh Token を設定します。
アドレスフィルタ	—	IP もしくは CIDR を設定します。

6.1.4 Excel ファイルからインポート

スタティッククレデンシャルに限り、Excel ファイルから一括でインポートすることが可能です。一つ前の節でスタティック設定のための画面を開いた時点で、手動で登録を追加する代わりに以下の手順に従ってください。

 をクリック後、「インポート用ファイルをエクスポート」を選択し、インポート用ファイルをエクスポートします。

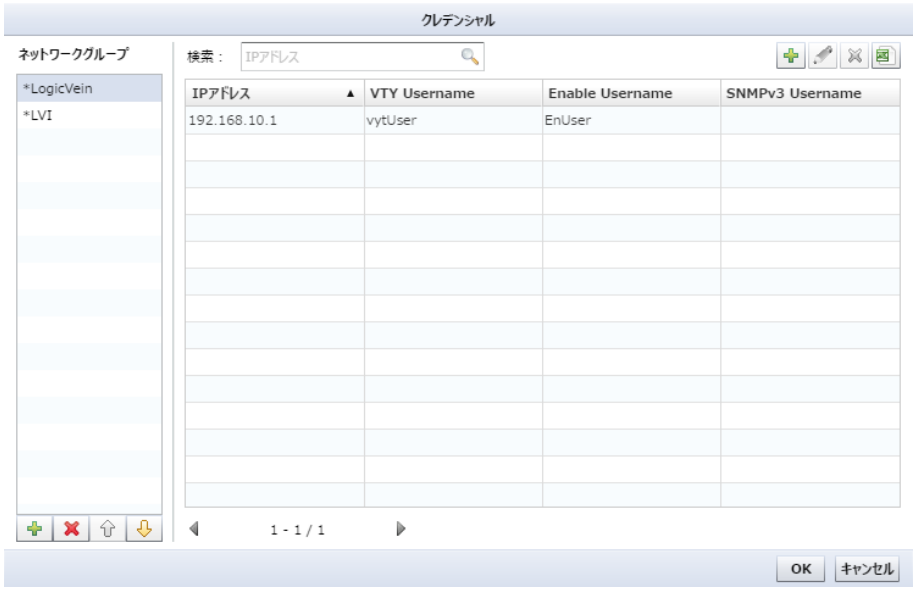


エクスポートされたファイルを Excel で開き、IP ごとにクレデンシャル情報を記入し保存します。入力が終わったら、ファイルを保存して netLD の画面に戻ってください。

入力例：

	A	B	C	D	E	F	
1	IP Address	VTY Username	VTY Password	Enable Username	Enable Secret/Password	SNMP Get Community	SNMPv3 Au
2	10.0.0.1	lvi	lvi123	enable	enable123	public	
3	10.0.0.2	lvi	lvi124	enable	enable124	public	
4	10.0.0.3	lvi	lvi125	enable	enable125	public	
5	10.0.0.4	lvi	lvi126	enable	enable126	public	
6	10.0.0.5	lvi	lvi127	enable	enable127	public	
7	10.0.0.6	lvi	lvi128	enable	enable128	public	
8	10.0.0.7	lvi	lvi129	enable	enable129	public	
9	10.0.0.8	lvi	lvi130	enable	enable130	public	
10	10.0.0.9	lvi	lvi131	enable	enable131	public	
11	10.0.0.10	lvi	lvi132	enable	enable132	public	
12							
13							
14							

 をクリック後、「クレデンシャルをインポート」を選択し、編集した Excel ファイルをインポートします。



エクセルファイルからデータを読み込む場合、同じ IP を持つ要素は上書きされてしまいます。インポートの際に意図しない上書きが無いよう、気をつけてください。

6.1.5 SSH 秘密鍵認証

SSH 秘密鍵認証により、デバイスのバックアップ、コンフィグ管理、およびターミナルセッションでパスワード認証の代わりに鍵認証を使用することができます。クレデンシャルセットで SSH 秘密鍵認証が設定されている場合、以下の状況において、その秘密鍵を使用してデバイスとの認証を行います。

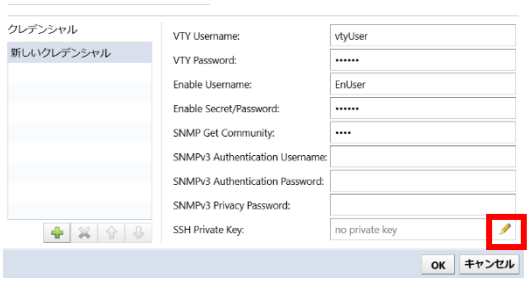
- バックアップ、復元
- ターミナルプロキシ
- ツール実行

秘密鍵とパスワードの両方が設定されている場合、まず鍵ベースの認証を試み、鍵が拒否された場合はパスワード認証に切り替えます。

備考	SSH 鍵認証を使用する際は、認証を正常に行うために、対象デバイス上で対応する公開鍵が適切に設定されていることを確認してください（authorized_keys ファイル）。 デバイス上で公開鍵が正しく設定されていない場合、認証は失敗し、パスワードが設定されている場合はパスワード認証に切り替わります。

6.1.5.1 SSH 秘密鍵の設定

クレデンシャルでユーザ名を設定後、SSH Private Key フィールドを選択してください。これは読み取り専用フィールドで、鍵が存在する場合、検出された鍵の種類が表示されます。SSH 秘密鍵を追加または変更するには、フィールドの右側にある鉛筆アイコンをクリックします。



これにより、SSH キーエディタダイアログが開きます。SSH 秘密鍵を設定する際は、必ずヘッダー行とフッター行を含めてください。パスフレーズを設定する際、秘密鍵がパスフレーズで暗号化されている場合は、パスフレーズ欄に入力してください。鍵がパスフレーズで保護されていない場合は、その欄を空欄のままにしてください。

項目	説明
SSH Private Key	秘密鍵ファイルの内容を全てテキストエリアに貼り付けます。
Passphrase	秘密鍵のパスフレーズを設定します。

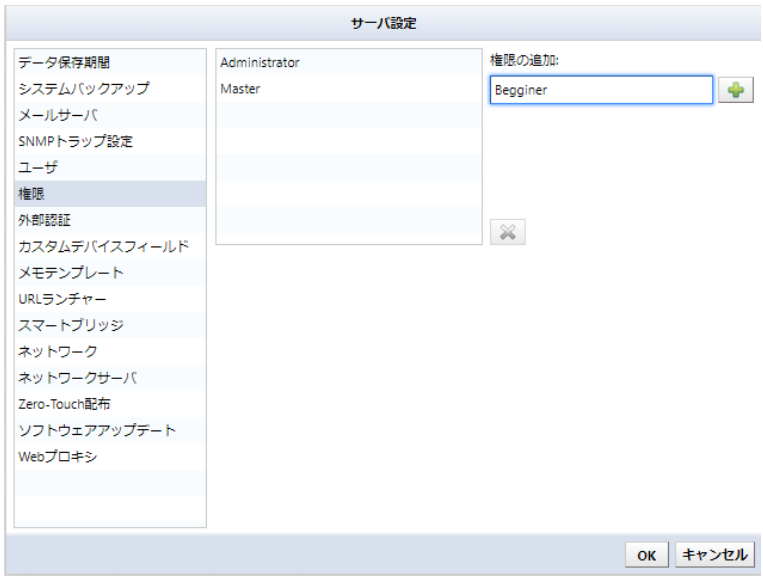
「OK」をクリックして保存するか、「キャンセル」をクリックして変更を破棄します。鍵が設定されている場合、「SSH 秘密鍵」フィールドには、鍵の内容そのものではなく、検出された鍵の種類が表示されます。

6.2 ユーザと権限の概要

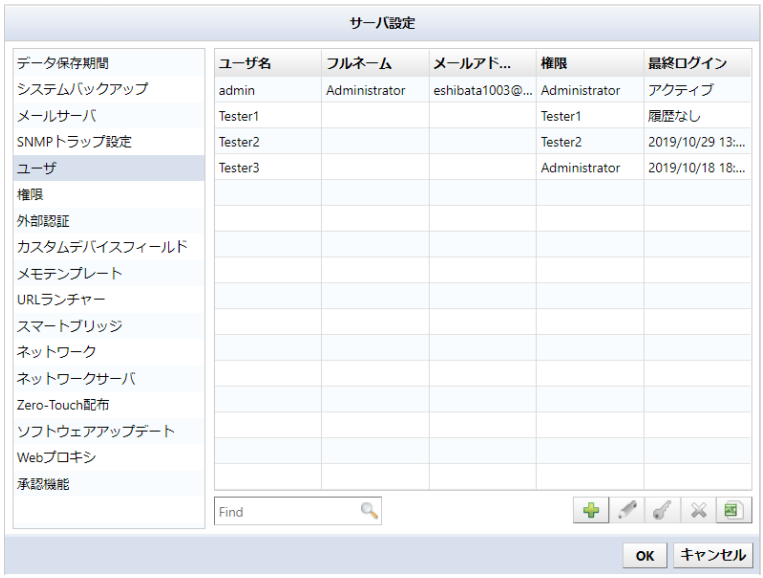
ユーザと権限は、*権限*がユーザの実行できる操作の範囲を指定し、それぞれのユーザに異なる権限を与えることができます。 それぞれの権限は、個別の操作に関する権限を集めたもので、個別の操作の例としては、例えば、デバイスの読み書き操作などがあります。

6.2.1 権限の作成

*サーバ設定ウィンドウ→権限*を開きます。*権限の追加*欄に新しい名前を追加し、  を押してください。



新しい権限が追加されました。表示されているチェックボックスをクリックして、その権限で許される操作を選択してください。



以下は設定できる権限の一覧表です。

項目	説明
1	コンプライアンスルールセットとポリシーの閲覧を許可する。
2	コンプライアンスポリシーの作成/更新/削除を許可する。
3	コンプライアンスルールセットの作成/更新/削除を許可する。
4	コンフィギュレーションの閲覧を許可する。
5	クレデンシャル及びプロトコル設定を許可する。
6	インベントリ内デバイス情報の作成/更新/削除を許可する。
7	カスタムフィールド名の設定を許可する。
8	インベントリ内デバイスへのタグ適用、解除を許可する。
9	ドラフトコンフィギュレーションの閲覧を許可する。
10	ドラフトコンフィギュレーションの作成/更新/削除を許可する。
11	スケジュールのフィルタ設定を許可する。
12	バックアップジョブの実行を許可する。
13	バックアップジョブの作成/更新/削除を許可する。
14	ディスカバリの実行を許可する。
15	ディスカバリジョブの作成/更新/削除を許可する。
16	スケジュールのフィルタ設定を許可する。
17	バックアップジョブの実行を許可する。
18	バックアップジョブの作成/更新/削除を許可する。
19	ディスカバリの実行を許可する。
20	ディスカバリジョブの作成/更新/削除を許可する。
21	ツールの実行を許可する。
22	ツールの作成/更新/削除を許可する。
23	ツールの実行を承認する権限。
24	承認なしにツールを実行する権限。
25	バルクチェンジジョブの実行を許可する。
26	バルクチェンジジョブの作成/更新/削除を許可する。
27	デバイスコンフィギュレーション変更ツールの実行を許可する。
28	レポートの実行を許可する。
29	レポートの作成/更新/削除を許可する。
30	コンフィギュレーション復元ジョブの実行を許可する。
31	ネイバー情報収集ジョブの実行を許可する。
32	ネイバー情報収集ジョブの作成/更新/削除を許可する。
33	URL ランチャーの作成/更新/削除を許可する。
34	レポートの実行を許可する。
35	レポートの作成/更新/削除を許可する。
36	コンフィギュレーション復元ジョブの実行を許可する。
37	ネイバー情報収集ジョブの実行を許可する。
38	ネイバー情報収集ジョブの作成/更新/削除を許可する。
39	URL ランチャーの作成/更新/削除を許可する。
40	メモの作成/更新/削除を許可する。
41	管理ネットワークの作成/更新/削除を許可する。

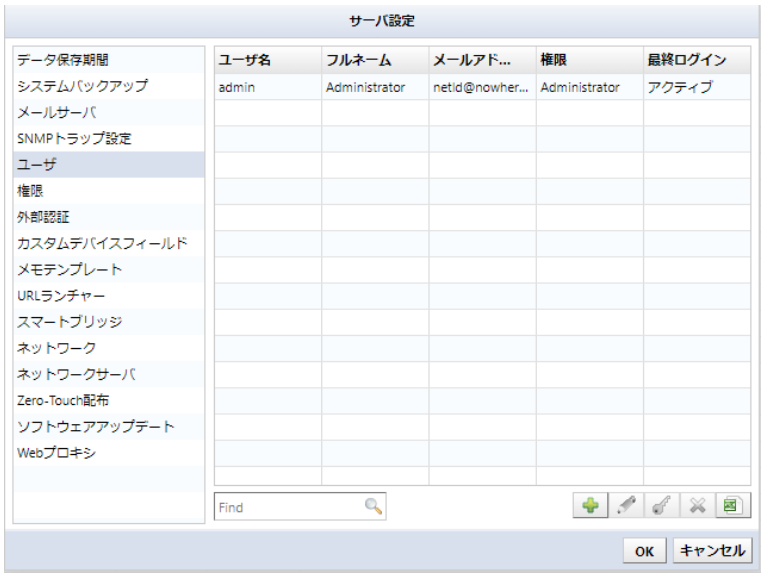
項目	説明
42	Zero-Touch コンフィギュレーションの作成/更新/削除を許可する。
43	Zero-Touch テンプレートの作成/更新/削除を許可する。
44	セキュリティの設定を許可する。
45	インベントリタグの作成/更新/削除を許可する。
46	ターミナルサーバ プロキシ経由でのログインを許可する。
47	ターミナルサーバ プロキシ経由での自動ログインを許可する。
48	enable mode に直接ログインを許可する。
49	他のユーザのターミナルアクセスログ閲覧を許可する。

※　権限には、依存関係のあるものがあります。

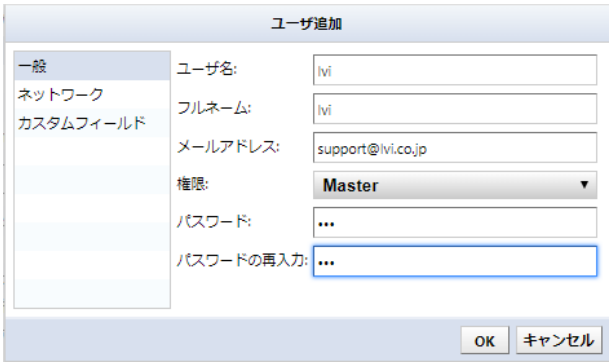
※　使用しているライセンスによっては、一部表示されない権限項目があります。

6.2.2　ユーザの設定

再び、*サーバ設定ウィンドウ→ユーザ*を開き、 を押してください。

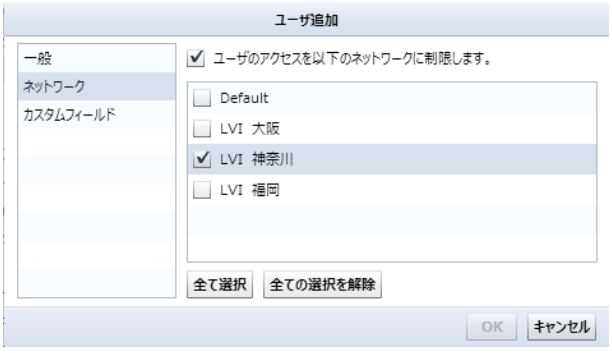


一般項目からは、ユーザごとに複数の要素を設定することができます。

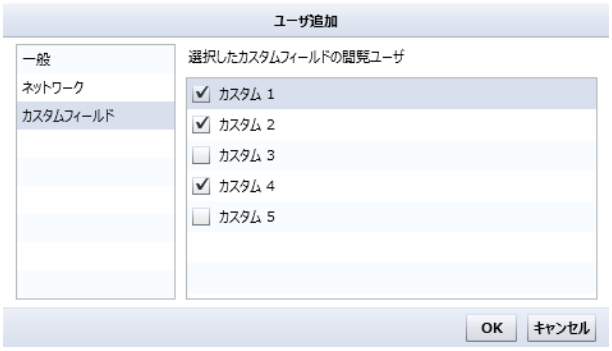


項目	説明
ユーザ名	ユーザの netLD へのログイン名を指定します。
フルネーム	ユーザの本名を入力します。
メールアドレス	ユーザの E-mail アドレス
権限	ユーザの権限をドロップダウンリストから選びます。
パスワード	ログインパスワードを入力します。
パスワードの再入力	確認のため同じパスワードを再入力します。

*ネットワーク*項目からは、ユーザのアクセスできる*ネットワーク*を制限することが出来ます。制限を加えるには、*ユーザのアクセスを以下のネットワークに制限します。*チェックボックスをオンにし、続いて、このユーザがアクセスできるネットワークをオンにしてください。



*カスタムフィールド*項目では、同様に、カスタムフィールドへの閲覧権限を設定できます。ユーザは、オンになったカスタムフィールドのみ閲覧することが出来ます。



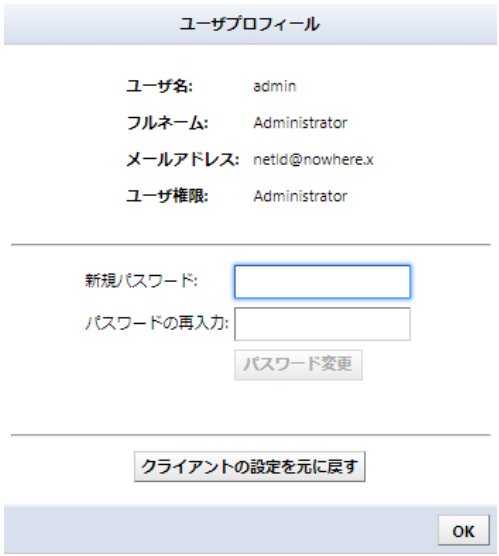
作成したユーザを保存するには、OK ボタンを押してください。

6.2.3 自分のパスワードを簡単に変更する

ログイン中であれば、自分のパスワードに限り、変更する方法があります。

グローバルメニューにある自分のログインユーザ名を押してください。下の例では、ユーザ名は admin で、これが*ログアウト*という項目の左に表示されています。

新たなパスワードを*新規パスワード*と*パスワードの再入力*フィールドに入力してください。*パスワード変更*ボタンを押すと、新しいパスワードが登録されます。



6.2.4　二要素認証（2FA）を設定する

リビジョン 20240905.2154 から、二要素認証を設定できるようになりました。二要素認証は、パスワードに加えて認証アプリによる追加認証を行うことで、ユーザアカウントのセキュリティを強化する機能です。ユーザは任意で設定できるほか、管理者はすべてのユーザに対して必須に設定することもできます。

6.2.4.1　二要素認証を有効にする

ユーザがログインしている場合、［ユーザプロフィール］ダイアログから二要素認証を設定できます。

1. ユーザ名をクリックし、［ユーザプロフィール］ダイアログを開きます。
2. ［二要素認証を設定］をクリックします。

3. 画面上の指示に従って設定を行い、認証コードを入力します。

4. ［OK］をクリックします。

以上で設定は完了です。ログアウト後、再度ログインすると、認証コードの入力が求められるようになります。

6.2.4.2 二要素認証を解除する

二要素認証の設定を解除したい場合、ログイン中のユーザ自身で解除することができます。また、admin ユーザの場合は、すべてのユーザの二要素認証の設定を解除することができます。

1. ［設定］>［ユーザ］を開きます。
2. 対象のユーザを選択し、［鍵］ボタンをクリックします。
3. ［二要素認証を解除する］にチェックを入れ、［OK］をクリックします。
   ※ 二要素認証が設定されていない場合は、「このユーザには二要素認証が設定されていません」と表示され、このチェックボックスオプションは表示されません。
4. ［サーバ設定］ダイアログで［OK］をクリックします。

6.3 デバイスの追加

デバイスは、追加、変更、削除、バックアップ、タグ付、検索、といった様々な操作を行うことができます。 この中でも最も重要な機能は、デバイスの追加です。チュートリアルで触れたとおり、netLD インベントリへのデバイスの追加には、2 つの方法があります。

- 自動ディスカバリによる追加
- 手動でのデバイス追加

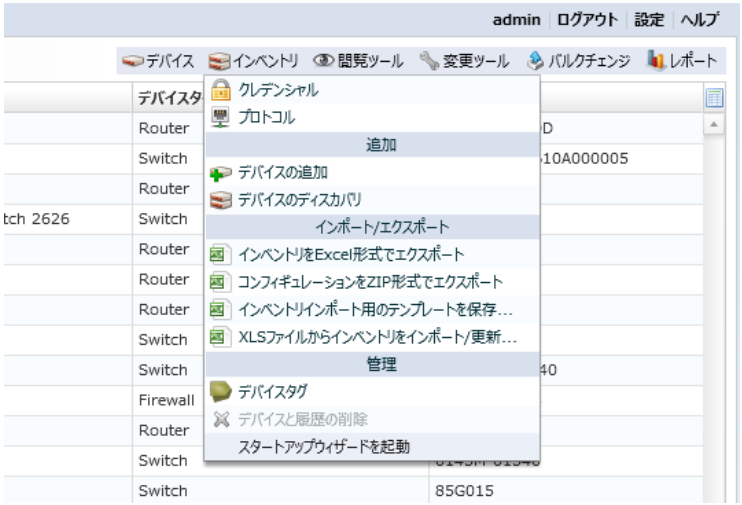
自動でデバイスを追加するためには、netLD だけでなくデバイスも、事前に適切に設定されている必要があります。ディスカバリがうまく行かない場合には、以下の条件をもう一度ご確認ください。

- お使いのデバイスが SNMP に対応しており、かつそのデバイスの設定で SNMP 機能がオンになっていること。
- クレデンシャルに関する情報がすでに入力されていること。
- netLD の用いるポートが、その他のプログラム(ファイアウォールやアンチウイルスソフト）によってブロックされていないこと。netLD が用いるポートのリストは、「使用ポート一覧」にリストされています。
- 一度にディスカバリが可能な最大デバイス数は 66,000 となります。 この数値は、明らかにとても巨大な値です。企業単位のネットワークにおいては、十分な数値であると言えます。たとえば、10.2.*.* というアドレス範囲は、65,025 アドレスで構成されています。

デバイスを追加するためのどちらのメニューも、*ツールメニューの インベントリ→追加*セクションにあります。手動でデバイスを追加するのは *デバイスの追加*から、自動での追加は *デバイスのディスカバリ*から利用することが出来ます。

6.3.1 デバイスのディスカバリによる追加

デバイスディスカバリは、先程述べた複数の条件が満たされているならば、とても便利に使うことが出来ます。ディスカバリは以下のように行われます。まず netLD サーバは、ディスカバリ時に指定された IP 範囲の IP それぞれに対し、後の通信に用いるポート(SSH/Telnet)が開いているかどうかを確認します。確認に成功すると、SNMP でデバイスの情報を取得しインベントリに登録します。ディスカバリを実行するには、*インベントリ→追加→デバイスのディスカバリ*を押し、以下の手順に従ってください。



まず、探索を行うすべての IP アドレス範囲を指定します。左のメニューから IP アドレス範囲を入力し、  を押してください。 追加された範囲はウィンドウ下部の一覧に表示されます。

項目	説明
IP アドレス/CIDR	IP アドレス範囲にサブネットマスクを用いて指定します。 (例: 192.168.0.1 /24)
IP アドレス範囲	2 つの IP アドレスを入力し、その間のアドレスが対象になります。

項目	説明
	(例: 10.0.0.1 –10.0.0.100)
IP アドレス ワイルドカード	IP アドレス範囲にワイルドカードマスクを用いて指定します。 (例: 192.168.0.*)
単一の IP アドレス	IP アドレスをひとつ入力します。 (例: 192.168.0.1)
クラウドアカウントからのインポート	クレデンシャルで追加したクラウドアカウントのデバイスを自動的に検出、追加します。

アドレス範囲のデータはテキストファイルからインポートすることも出来ます。一行に一つ IP アドレスを入力し、これを読み込ませてください。

	A	B	C	D	E	F
1	10.0.0.1-10.0.0.10					
2	192.168.0.0/24					
3	172.16.0.1					
4						

画面のその他の要素の説明は以下のとおりです。

- 境界ネットワーク

ディスカバリの範囲を制限するため、境界ネットワークアドレスを入力してください。 デフォルトでは、10.0.0.0/8, 172.16.0.0./16,192.168.0.1/16,FD00::/8 がセットされています。このアドレスに収まらない範囲のデバイスを検索したい場合には、その追加の範囲をここに追加します。

- デバイスのルーティングテーブルを参照し、ディスカバリ対象を追加する

有効な場合、ディスカバリしたデバイスのルーティングテーブルを確認し登録されているネットワークもディスカバリ対象とします。

- 既に登録されているデバイスのルーティングテーブルを参照し、ディスカバリ対象を追加する

有効な場合、既に登録されているデバイスのルーティングテーブルを確認し登録されているネットワークもディスカバリ対象とします。

- 追加 SNMP コミュニティストリング

ディスカバリを行う際に、入力されたコミュニティストリングを優先して使用します。

最後に実行をクリックし、ディスカバリを開始します。ディスカバリが完了すると、管理対象デバイスがデバイスビューに表示されます。また、探索中は、ディスカバリ状況がステータスペインに表示されます。

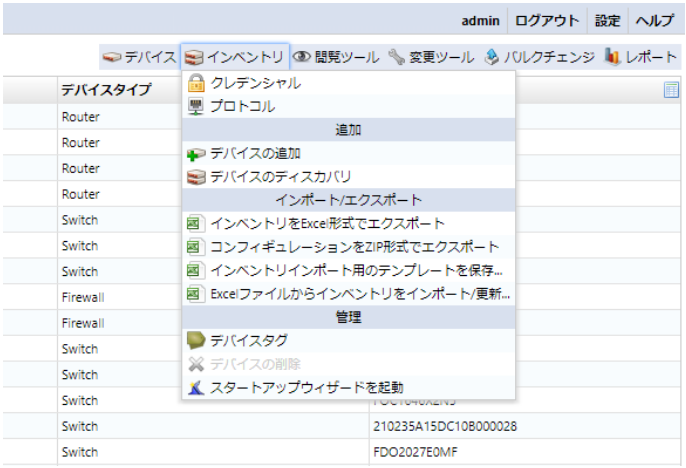
ディスカバリ結果として表示されるものは Telnet/SSH に返答したデバイスのみです。

ディスカバリ状況の詳細は以下のとおりです。

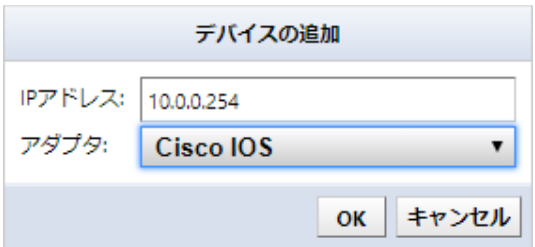
項目	説明
デバイスを追加しました。	ディスカバリが成功し、デバイスが netLD に追加された状態
SNMP 応答がありません。	Telnet や SSH、ping に応答があったが、SNMP 応答がない状態
一致するアダプタがありません。	SNMP 応答もあったが、netLD にアダプタが存在しない状態
サーバのプロトコル設定で、このデバイスの SNMP が無効になっています。	プロトコル設定にて、SNMP プロトコルのチェックが外れている状態
ICMP ping 応答がありません。	ICMP ping の応答がない状態(単一 IP アドレスでのディスカバリ時のみ)
ポート 22(SSH)と 23(Telnet)に TCP 接続できません。	ポート 22(SSH)と 23(Telnet)に TCP 接続できない状態(単一 IP アドレスでのディスカバリ時のみ)

6.3.2 手動でデバイスを追加する

デバイスは手動で追加することも出来ます。手動での追加は、*インベントリ→追加→デバイスの追加*から行えます。

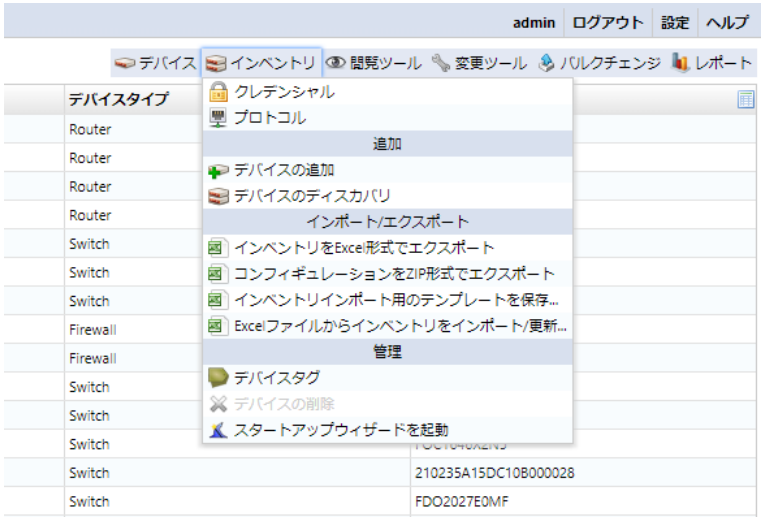


IP アドレスとアダプタ名を入力します。



項目	説明
IP アドレス	追加するデバイスの IP アドレスを入力します。
アダプタ	どの機種(アダプタ)のデバイスを追加するかを選んでください。

手動での追加方法にはもうひとつ、手書きしたエクセルファイルをインポートする方法があります。netLD はまた手書きエクセルファイルを書くために必要なエクセルテンプレートを出力することができます。出力するには、[インベントリ] → [インベントリインポート用のテンプレートを保存] を開きます。



出力されたエクセルファイルを編集し、保存します。

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	IP Address	Network	Adapter ID	Hostname	Type	Vendor	Model	OS Version	Serial Number	Memo	NWグルー	設置期	最終作業	設置拠点名	サービス
2	10.0.2.1	Default	Juniper ScreenOS	ssg5											
3	10.0.2.2	Default	NEC IX	IX2025_LVI	Router	NEC	IX2025	8.5.21	12TNU01048						
4	10.0.2.3	Default	Yamaha RT/RTX	RTX1200	Router	Yamaha	RTX1200	10.01.22	D26059822						
5	10.0.2.4	Default	Apresia	Apresia_LVI	Switch	Apresia	Apresia3424GT-SS	7.22.01							
6	10.0.2.5	Default	Cisco IOS	C3640	Router	Cisco	CISCO3640	12.3(11)T	26433110						
7	10.0.2.6	Default	D-Link DGS	DGS3426	Switch	D-Link	DGS-3426	2.62.B61	P1AJ1A20000040						
8	10.0.2.7	Default	Extreme Extremeware	Summit48i	Switch	Exterme	Summit48i	7.3.2.3	0145M-01450						
9	10.0.2.30	Default	Alaxala AXS	AX2430S	Switch	Alaxala	AX2430S-24T	10.4	85G015						
10	10.0.2.50	Default	Cisco IOS	LVI_Router	Router	Cisco	CISCO1841	15.1(1)T	FHK142172C3						
11															

項目	説明
IP アドレス(必須)	追加するデバイスの IP アドレスを記します。
ネットワーク(必須)	netLD に登録されているネットワーク(選択式)を選択します。
アダプタ ID(必須)	デバイスのアダプタ ID(選択式)を選びます。
カスタム 1～5	カスタムフィールド用の任意の情報を入力します。

最後に、[インベントリ] → [Excel ファイルからインベントリをインポート/更新] から、保存したファイルを再び netLD にインポートします。

6.3.3 クラウドアカウントのディスカバリ

クラウドクレデンシャルの追加に伴い、デバイスのディスカバリにおいて複数のクラウドアカウントを選択できるようになりました。インベントリからデバイスディスカバリを実行するのと同様に、ディスカバリジョブでクラウドアカウントを設定し、ディスカバリを実行する事ができます。

実行をクリックすると、設定されたクレデンシャルセットを使用して、指定されたディスカバリ境界内にあるデバイスを検出します。

6.3.4 デバイスを変更・削除するには

特定のデバイスの IP アドレスやホスト名、アダプタ、ネットワーク、カスタムフィールドを直接書き換えたいという場合には、デバイスビュー中のデバイスをクリックして選択し、*デバイス→デバイスプロパティの編集*を開いてください。デバイスを削除する場合には、デバイスを選択した状態で*インベントリ→デバイスの削除*を開いて削除をしてください。

6.4 デバイスの検索

デバイスの検索とは、検索条件に合致したデータのみを抽出して、デバイスビューに表示する機能です。インクリメンタルサーチに対応しているため、1 文字入力するたびに絞り込みが行われ、検索対象をすばやく見つけることができます。

検索対象は、表示中の管理ネットワークに属しているデバイスに制限されます。

6.4.1 IP アドレス/ホスト名を検索する

デバイス一覧の上部には、「IP/ホスト名検索」がデフォルトで表示されます。「IP/ホスト名検索」では、IP アドレスまたはホスト名を入力することでデバイスビューに表示するデバイスを絞り込むことが出来ます。

検索条件をクリックすると、検索ボックスが表示されます。

検索ボックスにキーワードを入力すると、検索条件に合致したデータのみが抽出され、表示されます。

6.4.2 検索条件を追加する

デフォルトで表示されている「IP/ホスト名検索」以外の条件で検索したい場合や、複数の条件に合致するデータを抽出したい場合には、検索条件を追加できます。

[検索条件の追加]ボタンをクリックし、検索条件を追加する項目を選択します。

追加された検索条件をクリックし、検索条件を指定します。

追加できる検索条件は、以下のとおりです。

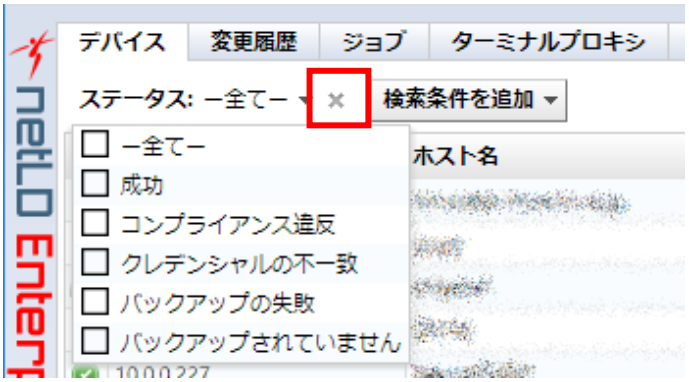
【検索条件一覧】

項目	説明
Interface IP	インタフェースモデル情報を含めて、IP アドレスを検索します。
Admin IP	デバイスビューの[IP アドレス]カラムから検索します。
ホスト名	デバイスビューの[ホスト名]カラムから検索します。
ステータス	バックアップステータスで検索します。
カスタム 1～5	[カスタム]カラムから検索します。

項目	説明
タグ	デバイスに割り当てられたタグから検索します。AND・OR 条件を組み合わせることができます。
メーカ・モデル・OS バージョン	デバイスのハードベンダーが表示されます。
シリアル番号	シリアル番号で検索をします。
MAC	MAC アドレスで検索しますが、完全一致した場合のみ表示されます。
コンフィグテキスト	デバイスコンフィギュレーションに対して全文検索を行います。詳細は右側の をクリックすると表示されます。

6.4.3 検索条件を削除する

検索条件を削除する場合、検索条件の右側に表示される[×]印をクリックします。

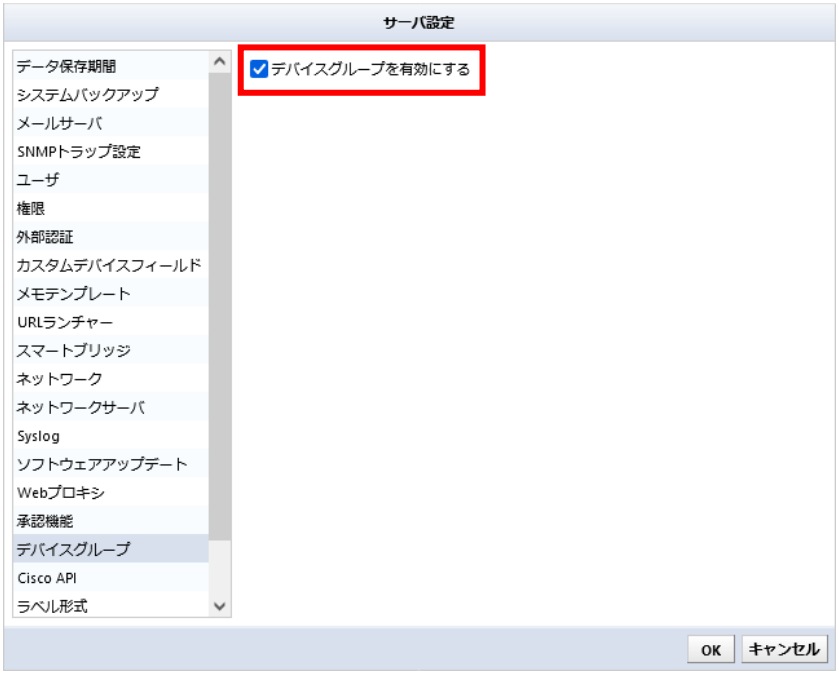


6.5　デバイスグループを使用する

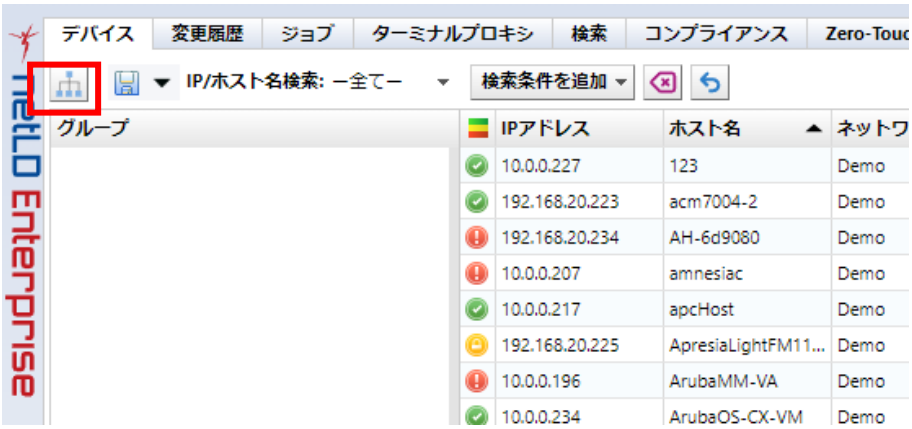
リビジョン 20240905.2154 から、デバイスグループを使用した検索ができるようになりました。デバイスグループとは、任意の条件でデバイスを分類できる機能です。すべてのユーザが共通して使用する「共有」グループと、各ユーザが個別に使用する「プライベート」グループを設定できます。また、階層的なグルーピングにも対応しており、より柔軟な管理ができます。

6.5.1　デバイスグループを有効にする

デバイスグループ機能は、デフォルトで無効になっています。デバイスグループを有効にするには、［サーバ設定］→［デバイスグループ］メニューで「デバイスグループを有効にする」にチェックを入れ、［OK］をクリックします。



デバイスタブにデバイスグループのアイコンが追加されます。アイコンをクリックするとサイドバーが表示され、デバイスグループを構成することができます。

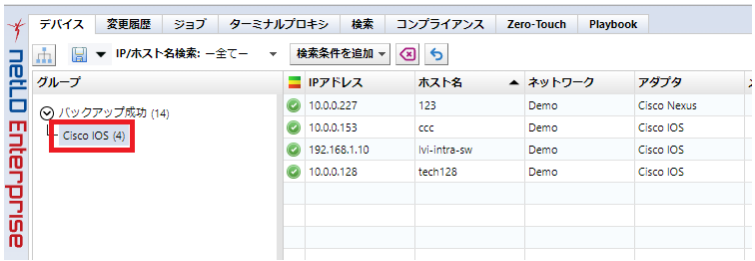


6.5.2　デバイスグループを追加する

デバイスグループを追加するには、グループサイドバーの左下にある［+］ボタンをクリックします。「名前」と「条件」を設定した後、［OK］ボタンをクリックします。なお、デバイスグループが最上位階層にある場合のみ、グループの「共有」または「プライベート」を選択できます。

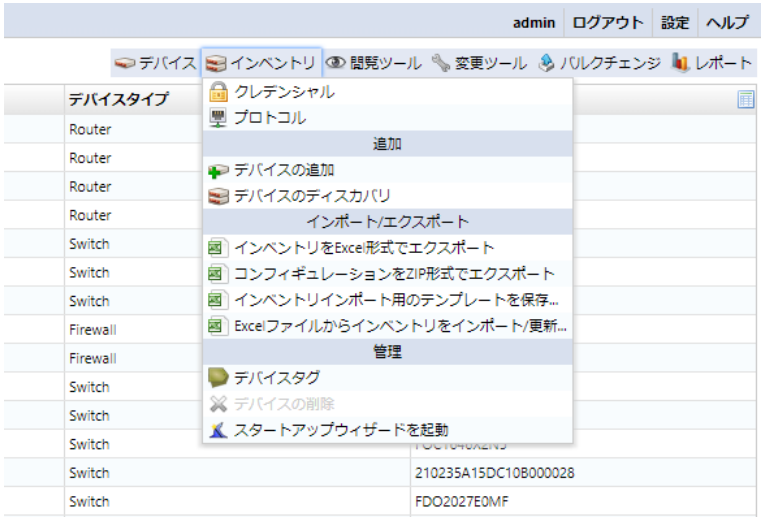
デバイスグループを追加すると、作成したグループがサイドバーに表示されます。デバイスグループを選択すると、インベントリ内のデバイスがその分類条件に基づいてフィルタリングされます。

デバイスグループは階層構造にすることができます。上位階層のグループを選択した状態で［+］ボタンをクリックすると、下位階層にグループを追加できます。ただし、下位階層のグループでは「共有」または「プライベート」を選択できません。



6.6　インベントリのインポートとエクスポート

現在のインベントリの状態をエクスポートまたは、インポートすることで一部の情報を更新することが可能です。これに関連する機能は、*インベントリ→インポート/エクスポート*セクションにあります。



- インベントリをエクセルファイルで保存する

この機能を用いると、一部のデバイス、あるいはインベントリのすべてのデバイスの情報をエクセルファイルとして保存することが出来ます。一部のデバイスのみをエクスポートする場合には、機能を使う前にそのデバイスを選択してください。 全体をエクスポートする場合には、何もデバイスを選択しないでください。その状態で*インベントリを Excel 形式でエクスポート*というメニュー項目を開き、保存するカラムにチェックを入れ「OK」ボタンをクリックします。

- エクスポートしたファイルをインポートしなおす

出力したファイルを再びインポートすることも可能です。そのためには、*Excel ファイルからインベントリをインポート/更新*を押してください。ただし、すべての項目がインポートできるわけではありません。インポートできる項目は IP アドレスとカスタムデバイスフィールドに限られます。

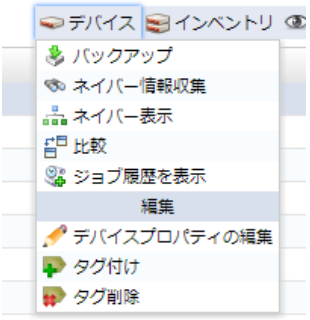
6.7　コンフィギュレーションとバックアップ

デバイスコンフィギュレーションのバックアップは、デバイスごとに異なるコマンドをネットワーク経由で実行することで行われます。 例えば IOS デバイスでは、以下のようなコマンドを用いることで現在のコンフィギュレーションを取得することが出来ます。

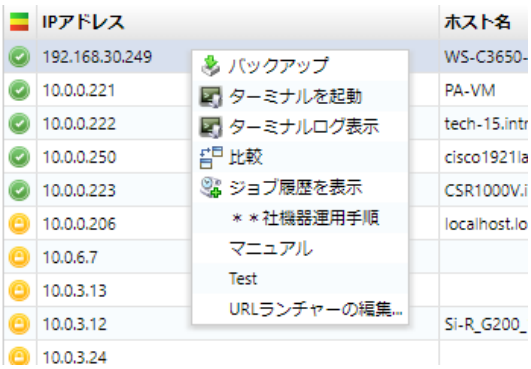
```
copy running-config tftp
copy startup-config tftp
show access-lists
show diag
```

netLD は、このようなコマンドのレシピを様々なデバイスについて持っており、そのレシピを用いて対象のデバイスをバックアップしています。レシピはメーカやモデルごとに異なるため極めて大量になります。大量のレシピを管理することは大変な作業です。仮に netLD を使わずにこの作業をそれぞれのネットワーク管理者に任せたとすると、たとえシェルスクリプトを用いて作業を自動化させたとしても、必要な作業は信じられない量に上ることが想像されます。

デバイスのバックアップを取るためには、単純にデバイス→バックアップボタンを押してください。特定のデバイスのみのバックアップを取りたい場合には、そのデバイスを選択した状態で同じバックアップボタンを押してください。



あるいは、デバイスを選択し、右クリックメニューからも個別のバックアップを行うことが出来ます。



バックアップが成功すれば、デバイスビューとインベントリが更新されます。各属性（IP アドレス、ホスト名、ハードベンダー、OS バージョン、シリアル番号等）に自動的に個別情報が収集され表示されます。

6.7.1 ステータスサマリ

ステータスペインに表示されるアイコンには、過去のバックアップの成功・失敗の報告が示されます。それぞれのアイコンには以下のような意味があります。

バックアップ失敗等トラブルシューティングに非常に役立ちます。

アイコン	説明
	バックアップに成功したが、前回バックアップしたものとデバイス上のコンフィギュレーションとの間に差分が検知された場合に表示されます。初回バックアップの際にも表示されます。
	バックアップ成功、変更なし。デバイス上のコンフィグデータが前回バックアップした内容と同じ場合に表示されます。
	クレデンシャルの不一致。登録されているクレデンシャルが誤っています。右に表示される結果をクリックすると、バックアップで使用したクレデンシャルが表示されます。インベントリ→クレデンシャルの設定を確認してください。
	失敗。コンフィギュレーションが取得できませんでした。アイコンをダブルクリックすると、詳細が表示されます。

6.7.2 バックアップ後のステータスについて

デバイスビューの左側に表示される、バックアップの実行結果を表すアイコンです。アイコンをダブルクリックすると、ステータス詳細が表示されます。トラブルシューティングに役立ちます。

アイコン	ステータス	説明
	バックアップ完了	コンフィギュレーション取得が完了しています。
	コンフィギュレーション不一致	デバイスの running-config と startup-config に差分があります。アイコンをダブルクリックすると、比較結果が表示されます。
	クレデンシャルの不一致	登録されているクレデンシャルが誤っています。アイコンをダブルクリックすると、バックアップで使用したクレデンシャルが表示されます。
	UNAVAILABLE_PROTOCOL	バックアップに必要なプロトコルでデバイスにアクセスできません。デバイスへの接続を確認し、*プロコトル*で必要なプロトコルのチェックが有効になっていることをご確認ください。
	UNEXPECTED_RESPONSE	デバイスから意図しない応答があった場合などに表示されます。問題が解決しない場合はサポートへお問い合せください。
	DEVICE_MEMORY_ERROR	デバイスに startup-config がありません。
	(その他)	その他のエラー。デバイスへの接続、クレデンシャル、プロトコルを確認し、問題が解決しない場合はサポートへお問い合せください。
	ワーニング	このデバイスは、障害度がワーニングに設定されたコンプライアンスポリシーに違反しています。
	エラー	このデバイスは、障害度がエラーに設定されたコンプライアンスポリシーに違反しています。

6.7.3 デバイスプロパティ

デバイスビュー内のデバイスをダブルクリックすることで、デバイスのハードウェア情報とバックアップ状況を確認することが出来ます。デバイスプロパティは、SNMP 経由やバックアップ、ネイバー情報取得などから netLD が獲得したハードウェア情報です。バックアップやネイバー情報検索を行えば、ここの情報は確実に最新の情報になります。

以下では、デバイスプロパティのサブタブを紹介します。

6.7.3.1 一般タブ

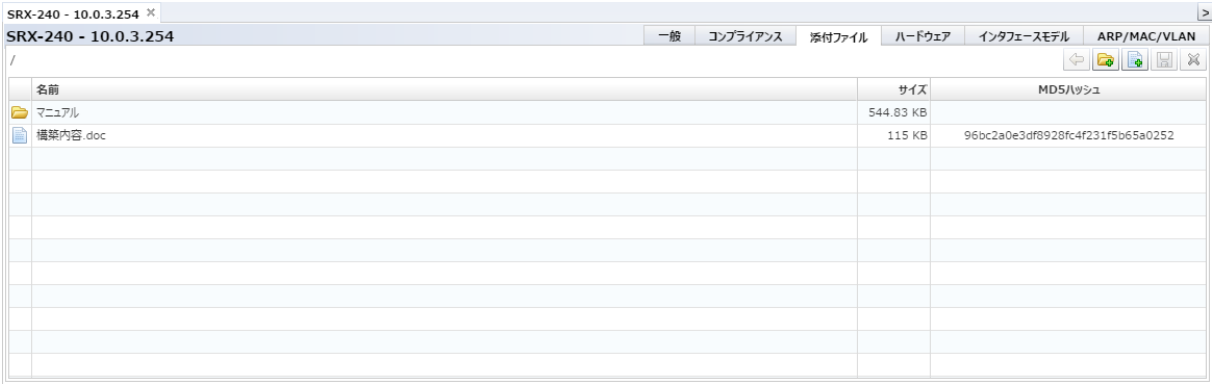
一般タブは デバイスのコンフィギュレーションや仕様を表示します。ここに表示される情報は最後のバックアップ時点の情報であるため、最新のものではない可能性があることに注意してください。

6.7.3.2 コンプライアンスタブ

コンプライアンスタブは、デバイスにコンプライアンス違反があった場合にその内容を表示します。詳細は、6.15 コンプライアンスの概要をご参照ください。

6.7.3.3　添付ファイルタブ

添付ファイルタブでは、任意のファイルを添付しておくことができます。デバイスのマニュアルなど構築内容を添付しておくと便利です。



6.7.3.4　ハードウェアタブ

ハードウェアタブは、デバイスのハードウェア情報をバックアップ時に収集された情報をもとに表示します。表示される例としては、ハードウェア構成やドーターカードのリスト、バージョンなどです。

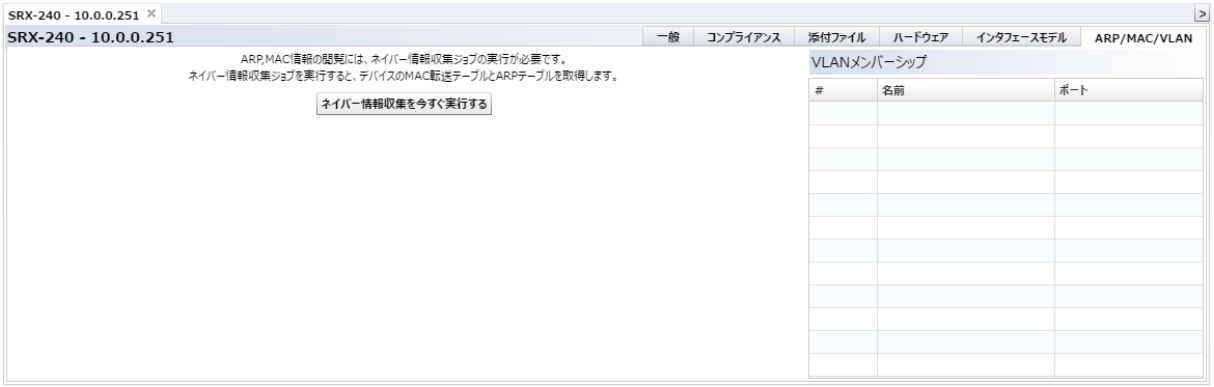
6.7.3.5　インタフェースタブ

インタフェースタブは、デバイスが備えるインタフェースについての情報を表示します。

6.7.3.6 ARP/MAC/VLAN タブ

ARP/MAC/VLAN タブはデバイス上の ARP テーブル, MAC テーブル、VLAN メンバーポート情報を表示します。この情報は、最後のネイバー情報調査ジョブ時点のデータです。

ネイバー情報収集前は、左のサブペインには何も情報が表示されません。ここにある*ネイバー情報を今すぐ収集する*ボタンを押すと、情報収集を簡単に実行することが出来ます。



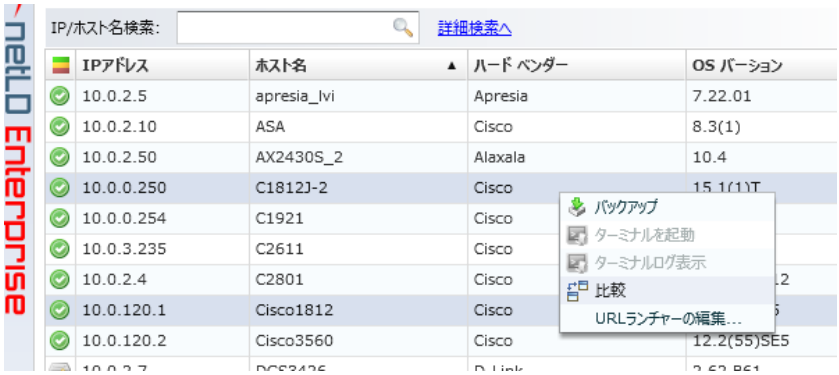
6.7.4 コンフィギュレーションの比較

コンフィグを比較する場合、2 つの使い方があります。同じデバイスの異なるコンフィギュレーションを比較する方法と、異なるデバイスのコンフィギュレーションを比較する方法です。

同じデバイスの異なるコンフィギュレーションを比較する場合、デバイスビューで 1 つのデバイスを選択し、［比較］メニューをクリックし、Ctrl キーを押しながら任意の 2 つのコンフィギュレーションを選択し、［比較］ボタンを押します。

異なるデバイスのコンフィギュレーションを比較する場合、デバイスビューで、Ctrl キーを押しながら任意の 2 つのデバイスを選択し、［デバイス］→［比較］メニューをクリックします。

あるいはデバイスビューを右クリックし、現れるメニューから*比較*を選択することも可能です。



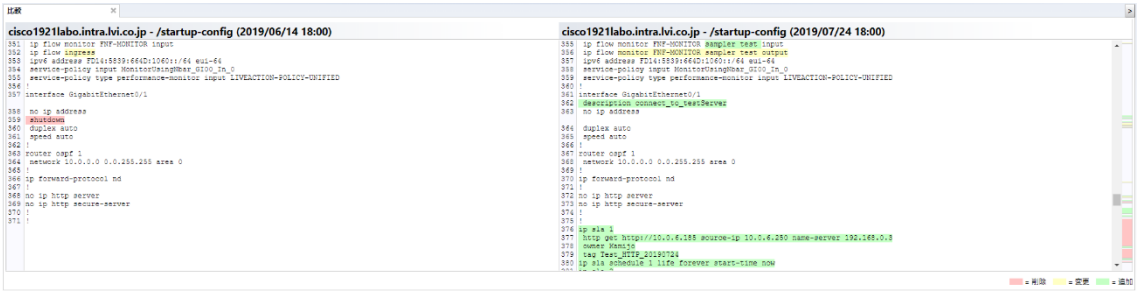
比較するコンフィギュレーションを選び、［比較］ボタンを押します。［コンフィギュレーション履歴の表示］にチェックを入れると、過去のコンフィギュレーションが同時に表示されます。

ステータスペインに開いたデバイス情報タブからコンフィグを比較することも出来ます。コンフィグ履歴から 2 つの項目を選択し、右上の  アイコンをクリックしてください。

コンフィギュレーションの比較結果が、色で強調表示されます。赤は削除された部分、黄色は変更された部分、緑は追加された部分です。

行単位ではなくコマンドレベルで比較されます。

更に、コンフィギュレーションコマンドが 1,000 行を越す場合も、右端の黒いバーを利用すると 1,000 行中の 854 行目（例）にジャンプして差分表示に素早く行きつけます。



6.7.5 startup-config と running-config の不一致を確認する

コンフィギュレーション不一致が通知されるのは、デバイスが 2 つのコンフィギュレーション, running-config と startup-config を持っていて、それらが異なる場合です。startup-config は、デバイスが再起動された直後に読み込まれるコンフィギュレーションで、通常の作業の場合これを用いるべきです。一方、running-config は一時的なコンフィギュレーションです。 だれかが startup-config を編集したのに再起動を忘れている場合、これはネットワークが正しく設定されていない状態につながります。 あるいは、ある変更が恒久的な変更であるべきだったのに、間違えてその変更を running-config だけに書きこんで編集してしまっていた場合、この変更は再起動の時に消えてしまうので、一度でも再起動が起こればネットワークは正しく設定されなくなってしまいます。

デバイスステータスがコンフィギュレーション不一致を示していた場合、アイコンをダブルクリックすれば、startup-config と running-config のコンフィギュレーション比較を表示することができます。右上のボタンを押せば、running-config を startup-config に書きこむか、あるいは running-config を startup-config に戻すかを選ぶことができます。

すべてのデバイスが running-config と startup-config の 2 つを持っているわけではありません。したがって、対応していないデバイスでは、netLD はアイコンを表示することはありません。

6.7.6 コンフィギュレーションを保存

収集したコンフィギュレーションは ZIP アーカイブ形式でデータを出力することもできます。この機能は、イベントリのメニューの*コンフィギュレーションを ZIP 形式でエクスポート*から使うことが出来ます。出力ファイル名は netLD-configs<エクスポート日時>.zip というフォーマットの名前になります。アーカイブ中のファイルは、以下のようなサブディレクトリに分けられて保存されます。

<filename>.zip
<network name>
10.0.0.1(1812J-B)
10.0.0.201(cisco2500b.intra.lvi.co.jp)
10.0.0.203 (cisco2600a.intra.lvi.co.jp)
10.0.0.208(C2801)
：

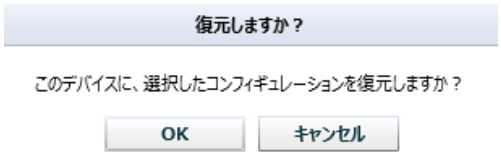
この機能は各機器の最新のコンフィギュレーションのみを出力できます。過去のコンフィギュレーションを出力したい場合には、デバイスプロパティの一般タブにて個々に保存します。保存したいコンフィギュレーションを選択しボタンを押してください。

6.7.7　コンフィギュレーションの復元

netLD では、故障した際、新規のデバイスに取得済みコンフィギュレーションを投入し、即復元を行うことが出来ます。

インベントリのデバイスをダブルクリックし、ステータスペインにバックアップ履歴を表示してください。復元するコンフィギュレーションを選び、  ボタンを押してください。

確認ダイアログで OK ボタンを押すと、コンフィギュレーションの復元を開始します。



この時点で netLD は、内部でデバイスにログインし、復元のコマンドを発行しています。多くの場合 TFTP や FTP を使用して選択した startup-config を書き戻し再起動することで、復元することができます。

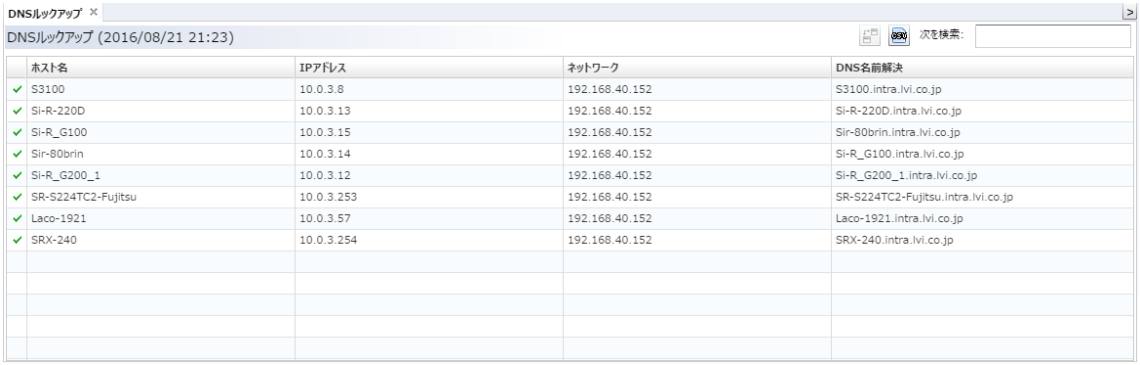
なお、コンフィギュレーションの復元では、自動的にデバイスの再起動が行われるため注意が必要です。

6.8 閲覧ツールの概要

*閲覧ツール*メニューから使用可能な機能は、選択したデバイスのリアルタイムの状況を知ることができます。検出された結果はまとめて CSV としてエクスポートすることも可能です。閲覧ツールを用いるときにはステータスペインに専用のタブが開かれるので、エクスポートは、そこの常に右上にあるボタンから行うことが出来ます。

6.8.1 DNS ルックアップ

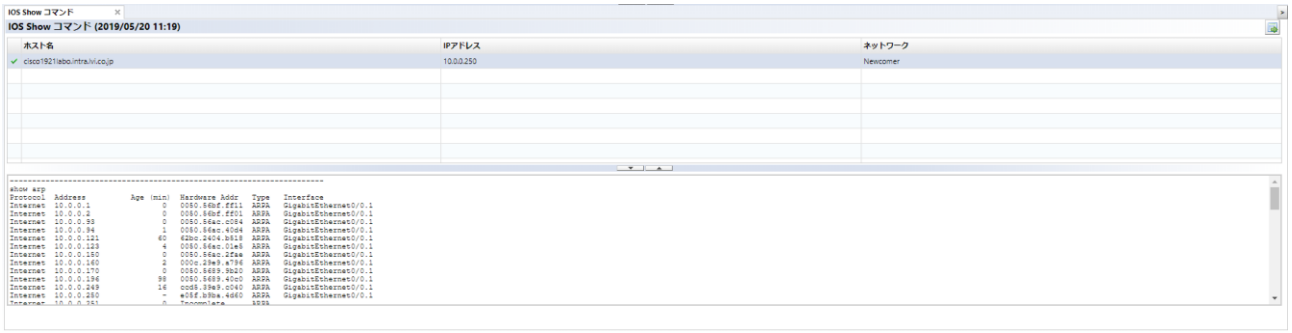
デバイスの DNS 名前解決情報を表示します。



6.8.2 IOS Show コマンド

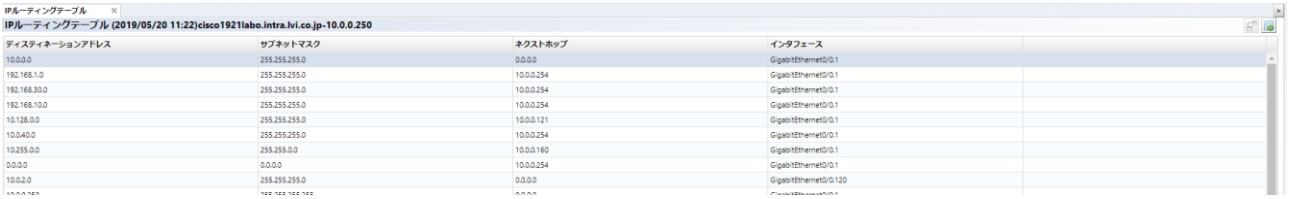
デバイスの IOS Show コマンドの結果を表示します。ただしこのコマンドは Cisco IOS と互換性のあるデバイス上でしか実行できません。はじめに実行する show コマンドをリストから選択し、*実行*を押すとコマンドが発行されます。

IOS Show コマンドを用いて、選択したデバイスに show arp コマンドを実行した際の結果画面が表示されます。



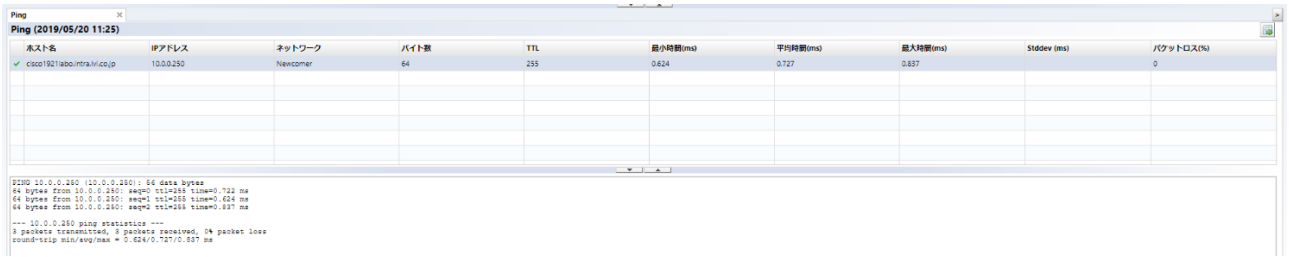
6.8.3 IP ルーティングテーブル

デバイスのルーティングテーブルを表示します。なお、この機能はデバイスを複数選択した状態では実行することができません。



6.8.4 Ping

デバイスに対して Ping を実行し、レスポンスを確認します。



6.8.5 SNMP システム情報

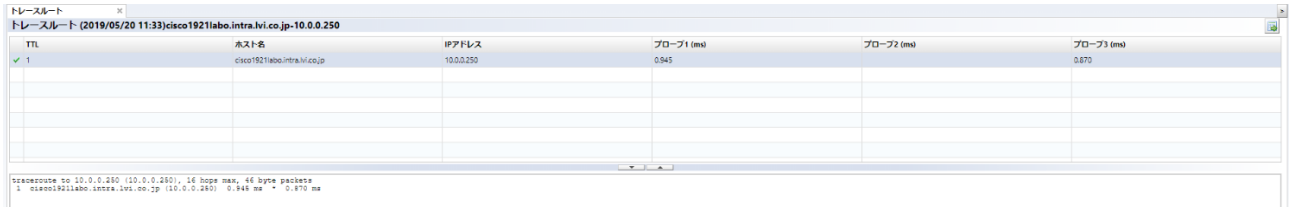
デバイスの SNMP システム情報を表示します。

6.8.6　インタフェース概要

デバイスの各インタフェースの開閉状態、IP アドレス等の詳細情報を表示します。なお、この機能はデバイスを複数選択した状態では実行することができません。

6.8.7　トレースルート

デバイスに対してトレースルートを行い、レスポンスを表示します。なお、この機能はデバイスを複数選択した状態では実行することができません。

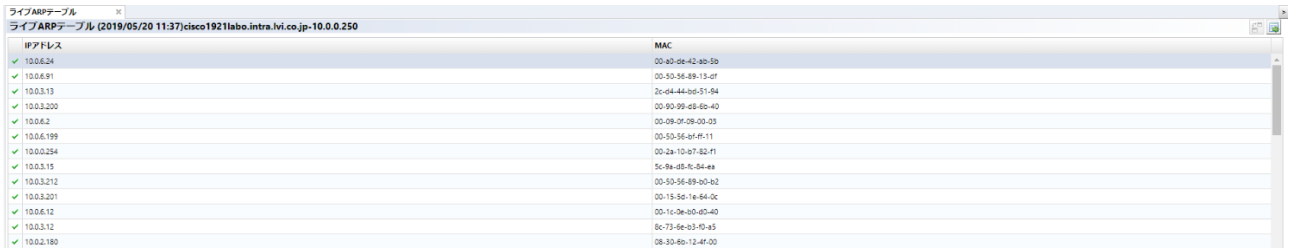


6.8.8　ポートマップ

デバイスのポート開閉情報を表示します。

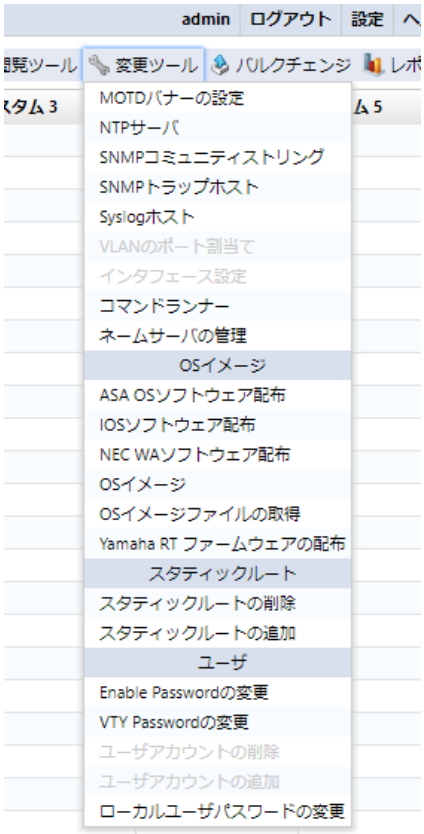
6.8.9　ライブの ARP テーブル

ARP テーブルのライブステータスを表示します。なお、この機能はデバイスを複数選択した状態では実行することができません。



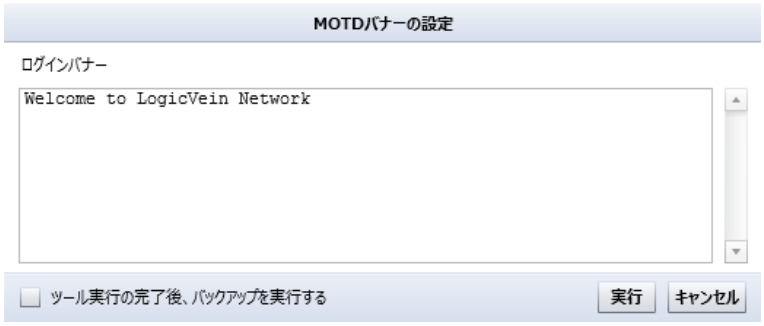
6.9 変更ツール

変更ツールサブメニューは、選択したデバイスのコンフィグを変更することに関連する操作を集めています。この章では、この変更ツールサブメニューにあるそれぞれの機能を上から順に解説していきます。



6.9.1 MOTD バナーの設定

デバイスのログインバナーを設定します。



6.9.2 NTP サーバ

NTP サーバをデバイスに追加/削除します。

6.9.3 SNMP コミュニティストリング

デバイスに対して、SNMP コミュニティを追加/削除します。

6.9.4 SNMP トラップホスト

デバイスに対して、SNMP トラップホスト設定を追加/削除します。NMS 新規導入の一括設定に威力を発揮します。

6.9.5 Syslog ホスト

デバイスに対して、Syslog ホストを追加/削除します。

6.9.6 VLAN のポート割当て

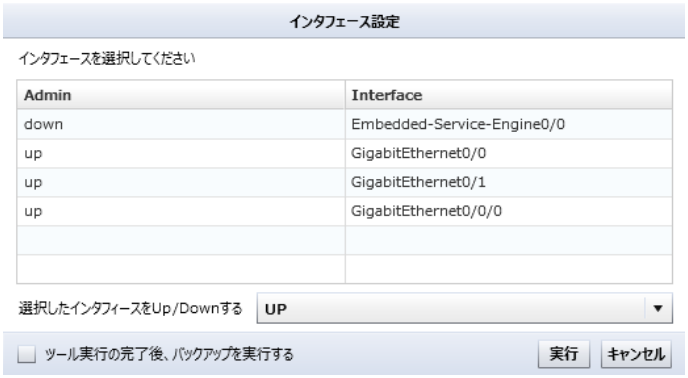
デバイスのアクセスポートに対して、VLAN ポートの設定を実行します。なお、この機能はデバイスを複数選択した状態では実行することができません。

画面のインタフェースを選択してくださいから、VLAN 設定対象のインタフェースを選択(複数選択可)し、VLAN を選択してください。欄から割り当てる VLAN を選択して OK ボタンをクリックします。

6.9.7　インタフェース設定

デバイスインタフェースの Admin Status を変更します。なお、この機能はデバイスを複数選択した状態では実行することができません。

「インタフェースを選択してください」欄から、Admin Status を変更するインタフェースを選択(複数選択可)し、プルダウンメニューで Up/Down を選択して「実行」ボタンをクリックします。



もし今あなたがそのデバイスに接続できる唯一のインタフェースを DOWN にしてしまった場合、それ以降そのデバイスにはリモート経由では接続できなくなってしまいます。運用には十分ご注意ください。

6.9.8　コマンドランナー

コマンドランナーは、複数のデバイスに同一の操作を繰り返し行う時に便利なツールです。たとえば、100 行以上のコマンドを沢山のデバイスに一度に実行できます。行うことのできるコマンドは、コンフィギュレーションのダウンロードやアップロードが含まれます。必要な項目を入力後、*実行*ボタンを押してください。

デフォルトの正規表現より優先するという欄は、特定のタイプのプロンプトにマッチする正規表現を指定します。マッチされるプロンプトは、シェルスクリプトで言えば PS1 変数のようなものです。この欄を指定する必要があるのは、あるコマンドが通常と異なるプロンプトを用いた返答をする場合です。たとえば、一部のインタラクティブなコマンドは通常『<username>#』で始まるプロンプトではなく、よりシンプルな『<』で始まるコマンドを用いて次の入力を促してくるかもしれません。その場合には、それを正規表現^< (行頭の<)で指定する必要があります。そうしなくては、コマンドの出力結果とプロンプトを区別することができなくなってしまいます。

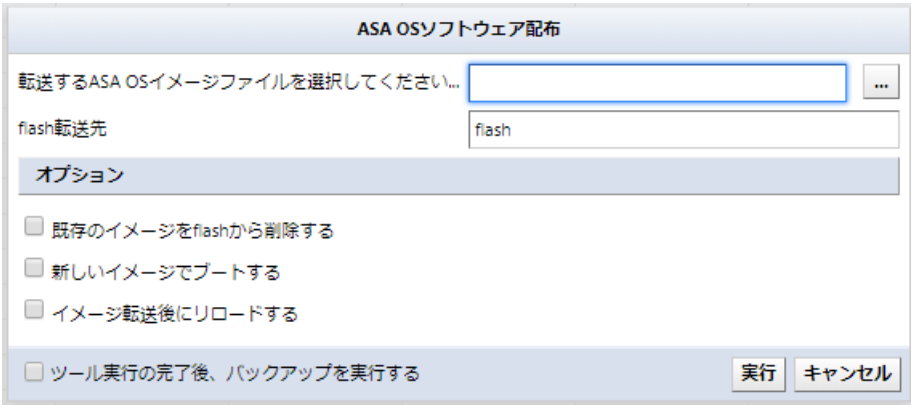
6.9.9 Allied Telesis OS ソフトウェア配布

Allied Telesis のデバイスに対して OS をリモート配布することができます。 本機能を使用するには、予め OS を保存しておく必要があります。 保存方法の詳細については 6.9.14 OS イメージを参照してください。

項目	説明
転送する OS イメージファイルを選択してください	右の[...]ボタンから、アップロードした OS イメージを選択します。
flash 転送先	デバイスの備える記憶ドライブを指定します。
flash ディレクトリ先	転送先ドライブ・パーティション内のディレクトリ。ディレクトリが存在しないときは、指定した名前のディレクトリが自動で生成されます。
既存のイメージを flash から削除する	指定されたディレクトリから既存のイメージを削除します。
新しいイメージでブートする	次にデバイスが再起動した時に、新しいイメージで起動するように設定します。
イメージ転送後にリロードする	イメージ転送後、デバイスを再起動します。
タイムアウト（デフォルト 300 秒）	ネットワークの通信遅延が多い環境で待機時間を指定する。

6.9.10 ASA OS ソフトウェア配布

Cisco ASA のデバイスに対して OS をリモート配布することができます。 本機能を使用するには、予め OS を保存しておく必要があります。 保存方法の詳細については 6.9.14 OS イメージを参照してください。



項目	説明
転送する ASA OS イメージファイルを選択してください	右の[...]ボタンから、アップロードした OS イメージを選択します。
flash 転送先	デバイスの備える記憶ドライブを指定します。
既存のイメージを flash から削除する	指定されたディレクトリから既存のイメージを削除します。
新しいイメージでブートする	次にデバイスが再起動した時に、新しいイメージで起動するように設定します。
イメージ転送後にリロードする	イメージ転送後、デバイスを再起動します。

6.9.11 IOS ソフトウェア配布

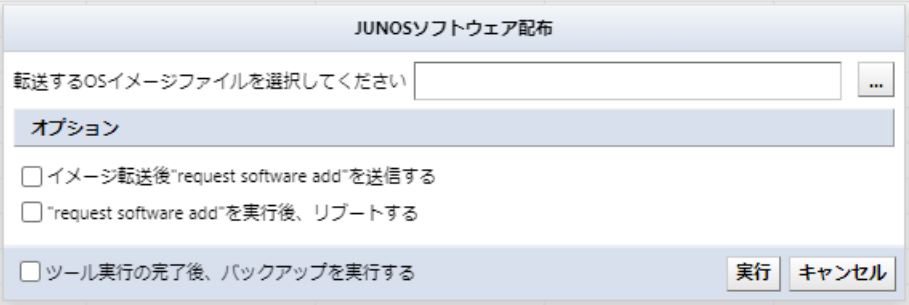
Cisco IOS のデバイスに対して IOS をリモート配布することができます。 本機能を使用するには、予め IOS を保存しておく必要があります。 保存方法の詳細については 6.9.14 OS イメージを参照してください。

項目	説明
転送する IOS イメージファイルを選択してください	右の[...]ボタンから、アップロードした OS イメージを選択します。
flash 転送先	デバイスの備える記憶ドライブを指定します。機種によって、flashusbflash0nvram など、指定できる内容が異なります。
flash ディレクトリ先	転送先ドライブ・パーティション内のディレクトリ。ディレクトリが存在しないときは、指定した名前のディレクトリが自動で生成されます。
flash パーティション先	転送先ドライブのパーティション。指定されたパーティションが存在しない場合にはコマンドは失敗します。
既存のイメージを flash から削除する	指定されたディレクトリから既存のイメージを削除します。
新しいイメージでブートする	次にデバイスが再起動した時に、新しいイメージで起動するように設定します。
イメージ転送後にリロードする	イメージ転送後、デバイスを再起動します。
メモリ要件の事前チェック(DRAM)	ツールを実行する前に、デバイスに十分なメモリ（DRAM）があるかどうかを確認し、十分でない場合はツールの実行を防止できます。

項目	説明
	http://cisco.com にて転送する IOS イメージに必要な DRAM 容量を確認し、その値を KB 単位で入力することを推奨します。

6.9.12 JUNOS ソフトウェア配布

JUNOS のデバイスに対して OS をリモート配布することができます。本機能を使用するには、予め OS を保存しておく必要があります。保存方法の詳細については「6.9.14 OS イメージ」を参照してください。



項目	説明
転送する OS イメージファイルを選択してください	右側の［…］ボタンを押すと、登録してある OS イメージをブラウズするウィンドウが現れますので、アップロードするイメージを選択してください。
イメージ転送後”request software add”を送信する	イメージ転送後、”request software add”を実行する。
”request software add”を実行後、リブートする	”request software add”を実行後、リブートする。

6.9.13 NEC WA ソフトウェア配布

NEC WA ソフトウェアをリモート OS 配布することができます。本機能を使用するには、予め WA ソフトウェアを保存しておく必要があります。保存方法の詳細については 6.9.14 OS イメージを参照してください。

項目	説明
転送する OS イメージファイルを選択してください	右の[...]ボタンから、アップロードした OS イメージを選択します。
既存のイメージを flash から削除する	flash から既存のイメージを削除します。

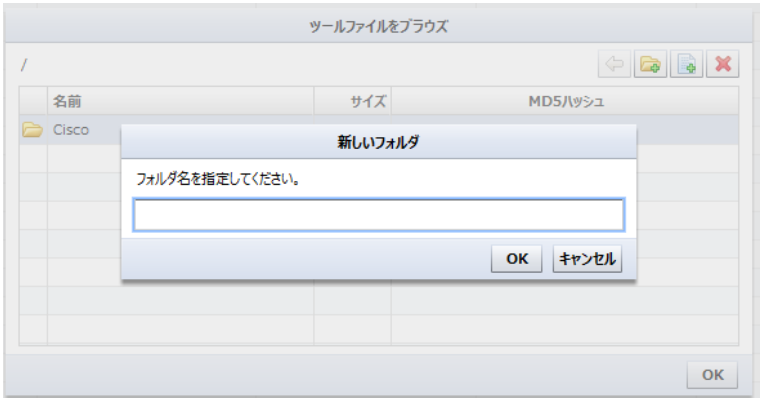
項目	説明
新しいイメージでブートする	次にデバイスが再起動した時に、新しいイメージで起動するように設定します。
イメージ転送後にリロードする	イメージ転送後、デバイスを再起動します。

6.9.14　OS イメージ

サーバのファイルシステム上のフォルダを指定し、そこからソフトウェア配布に使用するための OS イメージを検索し、データベースに登録します。

 ボタンを押し、OS イメージファイルを追加してください。

 ボタンを押すことで、ディレクトリを追加することもできます。このディレクトリの中から OS イメージが検索されます。

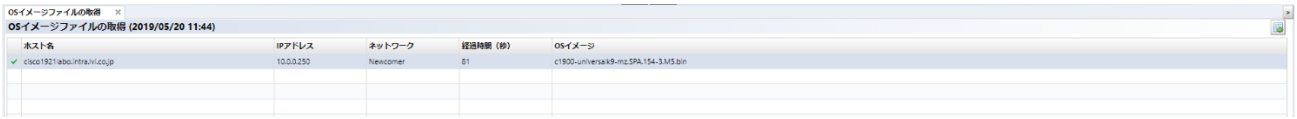


OS イメージが正しくリストに追加されたら、OK ボタンを押してください。

イメージを追加するのには多少時間がかかる可能性があります。もしあまりにも時間がかかっている場合や、追加されなかった場合には、指定するディレクトリを確認し、ファイル追加をもう一度やり直してみてください。

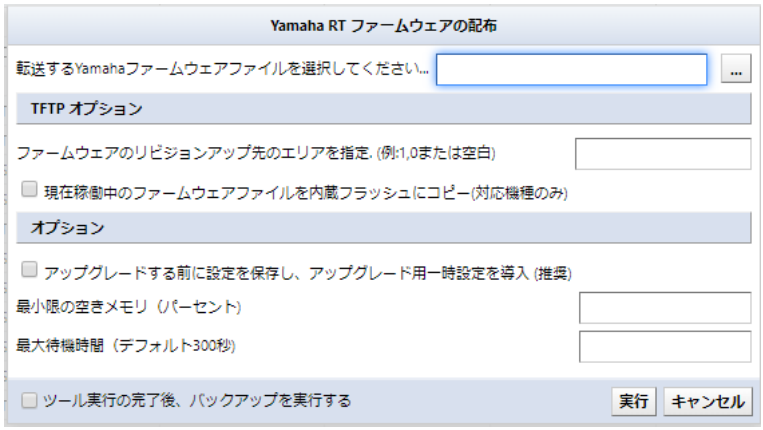
6.9.15 OS イメージファイルの取得

指定したデバイスから OS イメージをダウンロードしてデータベースに保存します。ダウンロードしたイメージは後に再びアップロードすることができます。



6.9.16　Yamaha RT ファームウェアの配布

Yamaha RT ソフトウェアをリモート OS 配布することができます。本機能を使用するには、予め Yamaha RT ソフトウェアを保存しておく必要があります。保存方法の詳細については 6.9.14 OS イメージを参照してください。



項目	説明
ファームウェアファイルを選択	対象のファームウェアファイルを選択
ファームウェアのリビジョンアップ先のエリアを指定	複数のファームウェアをサポートする機種では ROM エリア番号(1,0)を選択可能。指定しない場合は稼働中のファームウェアがアップグレードされる。
現在稼働中のファームウェアファイルを内蔵フラッシュにコピー	複数ファームウェアをサポートする機種で稼働中のファームウェアのバックアップを行う※1
アップグレードする前に設定を保持し、アップグレード用一時設定を導入	ファームウェアのアップロードを行う前に設定を保存して、コマンドを実行※2
最小限の空きメモリ	設定したメモリを超えた場合にファームウェアアップグレードを中止させることが可能※3
最大待機時間	ネットワークの通信遅延が多い環境で待機時間を指定
ツール実行の完了後、バックアップを実行する	ファームウェア配布時に Yamaha 機器はデバイスの仕様として再起動を行います。チェックを入れることでバックアップを実行しますが、デバイスの再起動中の為に失敗します。

※1: 以下の場合は Rev.14.01.14 が稼働中の為、このファームウェアのバックアップが行われます。

```
No.   Revision
-----+--------------------------------
  0   Rev.14.01.11
* 1   Rev.14.01.14
-----+--------------------------------
```

複数のファームウェアをサポートしない機種でこのチェックを行った場合、ファームウェアのアップグレートは中止されます。

また、リビジョンアップ先の ROM 番号と稼働中のファームウェアの ROM 番号が同じ場合にもアップグレードは中止されます。

※2: 下記のコマンドが実行されます。

login timer [timer]

show config | grep “tftp host”

tftp host [netLD IP]

※3: 以下のメモリ使用量の場合、80 を設定する事でファームウェアアップグレードは中止されます。

```
CPU:    0%(5sec)   0%(1min)   0%(5min)    Memory: 82% used↓
Packet-buffer:   0%(small)   0%(middle)   7%(large)   0%(huge) used↓
```

6.9.17　スタティックルートの追加

必要な情報を入力し、*実行*を押すと、ルートが追加されます。

6.9.18　スタティックルートの削除

既存のスタティックルート設定を選択して削除します。

6.9.19　Enable Password の変更

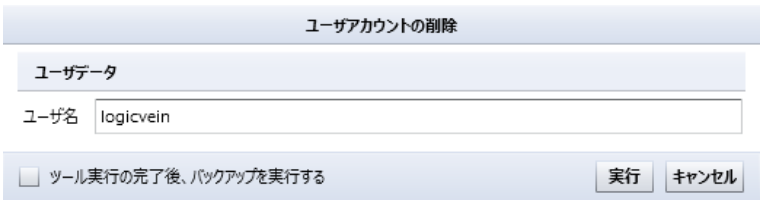
デバイスの Enable Password または Enable Secret の設定を変更します。Enable Password が設定されている場合は Enable Password が変更され、Enable Secret が設定されている場合は Enable Secret が変更されます。両方が設定されている場合は Enable Secret が変更されます。

6.9.20　VTY Password の変更

デバイスの VTY Password の設定を変更します。

6.9.21　ユーザアカウントの削除

デバイスに設定されている既存のユーザアカウントを削除します。なお、この機能はデバイスを複数選択した状態では実行することができません。



6.9.22　ユーザアカウントの追加

デバイスに新規ユーザアカウントを追加します。なお、この機能はデバイスを複数選択した状態では実行することができません。

6.9.23　ローカルユーザパスワードの変更

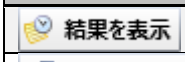
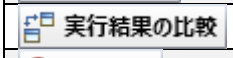
デバイスに設定されているユーザアカウントのパスワードを変更します。

6.10 ジョブ管理

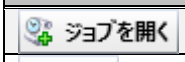
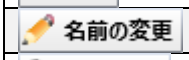
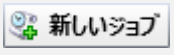
ジョブタブでは、ジョブを作成、編集、管理そして実行が出来ます。一つのジョブは、定期的に自動実行するように設定されたコマンドの集まりです。ジョブのトリガーとは、定期的な実行を引き起こすきっかけになる条件のことです。たとえば、1 月 1 日の正午，五分ごと，毎月の最初の月曜日などです。一つのジョブには複数のトリガーを与えることが出来、与えるトリガーを調整することで、ジョブを実行する頻度を制御できます。

ジョブタブは 2 つのサブタブ、ジョブ履歴タブとジョブ管理タブから成り立ちます。ジョブ履歴サブタブでは、過去のジョブ実行の結果を見ることが出来ます。自動的に実行されたものも手動で実行したものも、共にここに表示されます。

ジョブ履歴サブタブでは、以下のボタンがあります。

項目	説明
	選択したジョブの実行結果を開きます。
	選択した 2 つのジョブの結果を比較します。
	選択した実行中のジョブを中止します。
	ジョブ承認ログを表示します。

一方、ジョブ管理サブタブでは、ジョブの新規作成、作成済みジョブのプロパティ確認、編集などの実際の作業を行うことが可能です。登録されているジョブをダブルクリックすれば、編集画面が開きます。いくつかのボタンが提供されています。

項目	説明
	選択したジョブのプロパティを開きます。
	選択したジョブを削除します。
	選択したジョブの名前を変更します。
	選択したジョブを即時に実行します。
	新規ジョブを作成します。ツール/ディスカバリ/ネイバー/バックアップ/バルクチェンジ/レポートのジョブを追加できます。
	クーロン形式のフィルタを登録します。

6.10.1　ジョブの作成

ジョブは、ジョブ管理→新しいジョブ以下のサブメニューから作成できます。このサブメニューには様々な種類のジョブが登録されていますが、どの種類のジョブでもその作成の大まかな流れは変わりません。メニューから種類を選んだ後、ジョブを作るには、

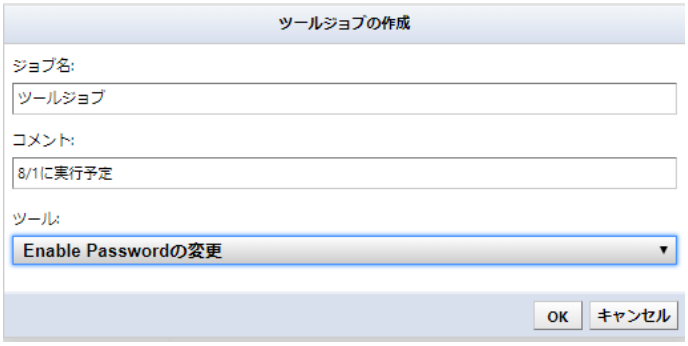
1. まずジョブ名を決め、使う機能を選びます。
2. 必要なパラメータを入力します。
3. 対象デバイスを選びます。
4. ジョブのトリガー(実行頻度)を入力します。

以下では、試しにジョブを一つ作り、その様子を画面ごとに実際に示して説明を行います。新しいジョブ→ツールをクリックしてみましょう。

6.10.1.1 ジョブ名を決め、機能を選ぶ

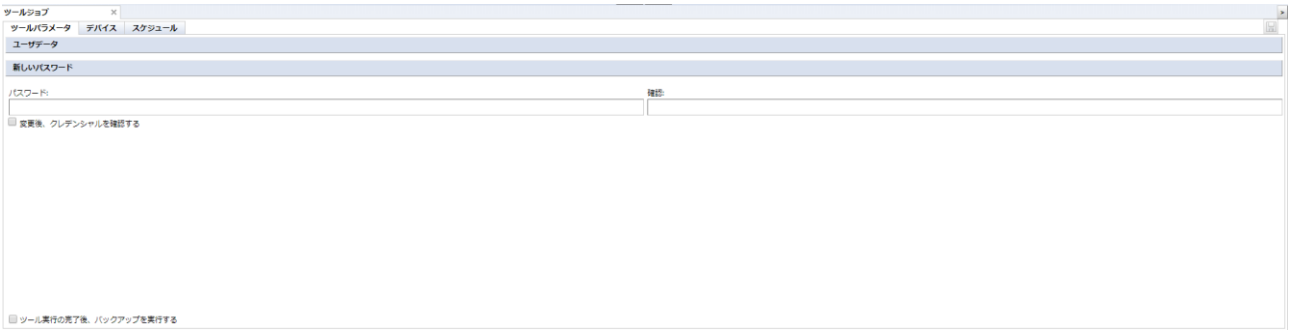
まずは、好きな名前でジョブ名を与えます。コメント欄には、後に他人がわかりやすいコメントを付け加えると良いでしょう。

次に、ツールを選びます。デバイスタブのツールメニュー→閲覧ツールと変更メニューで使うことのできるツールはほぼすべて選ぶことが出来ます。今回はイネーブルパスワードの変更を選んでみましょう。OK ボタンを押すと、ステータスペインに新しいタブが開かれます。



6.10.1.2 必要なパラメータを入力

次に、開かれた新しいタブで、必要なパラメータを入力します。(新しいタブは更にサブタブに別れており、ツールパラメータサブタブがデフォルトで開かれているはずです。)イネーブルパスワードの変更を選んだので、入力すべきツールパラメータはパスワード、確認、ツール実行の完了後、バックアップを実行します。



6.10.1.3 対象デバイスを選ぶ

画面のメインペインにはジョブタブが、ステータスペインには新しいジョブの設定タブ(その中にはツールパラメータサブタブ)が開かれているはずです。

ステータスペインでデバイスサブタブを選んでください。詳細検索機能と似た画面が表示されます。ただし、この画面には すべてのデバイス, 検索, 静的リストというラジオボタンがあります。

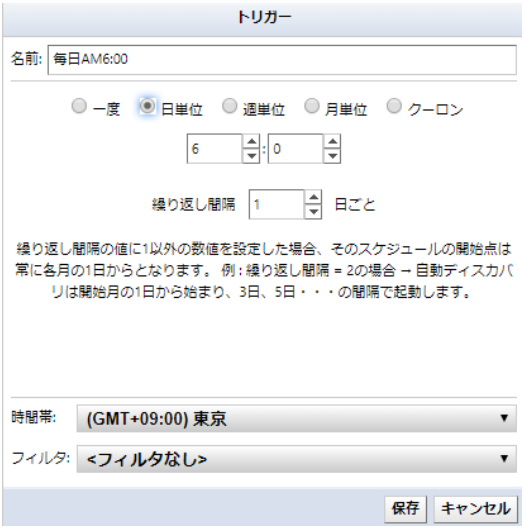
検索オプションを使う場合の注意としては、検索はジョブ実行時に行われるという事です。デバイスビューの検索で現れたものが固定されて追加されるのではありません。ジョブを実行するときに同じ条件で検索を行い、その結果に対してジョブを実行します。そのため、インベントリに新しいデバイスが追加され、かつそのデバイスがジョブ作成時の検索クエリにマッチした場合、ジョブはその新しいデバイスにも実行されます。この性質はうまく使えば便利ですが、間違えると想定外のデバイスにジョブを実行することになります。この点に留意してください。

6.10.1.4 トリガーを追加する

[スケジュール]タブでは、指定したスケジュールに基づいてジョブを実行するトリガーを設定することもできます。

左下の  ボタンをクリックし、新しいトリガーを追加します。

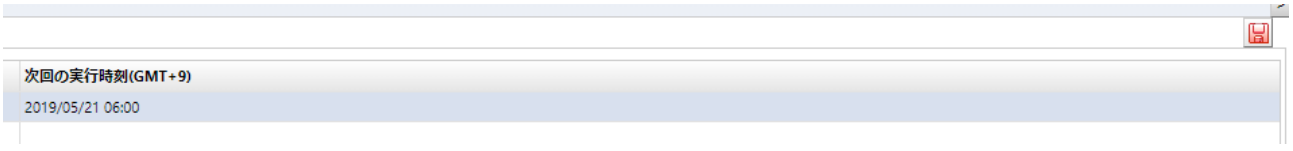
トリガーの名前を入力し、スケジュールを設定します。設定後、[保存]ボタンをクリックします。



項目	説明
名前	トリガーの名称
時刻	ジョブを実行する時刻、日付
スケジュール単位	以下 5 種類の実行スケジュールを選択 一度・・・時刻に設定されている日時に 1 度だけ実行する 日単位・・・n 日毎に実行する(起点は当月 1 日) 週単位・・・特定の曜日に実行する 月単位・・・指定した月毎に実行する クーロン・・・クーロン形式で指定した日時に実行する
時間帯	タイムゾーン
フィルタ	「フィルタの設定」で登録されているスケジュールフィルタを選択します。 このフィルタにマッチしたタイミングは、トリガーから取り除かれます。詳しくは、「スケジューラフィルタ」をご参照ください。

6.10.1.5 ジョブを保存する

最後に、右上にある  ボタンを押してジョブ設定を保存することを忘れないでください。



6.10.2 ジョブ履歴サブタブのジョブ実行ステータスの詳細

過去のジョブ実行は、そのジョブが成功したか失敗したかのステータスが記録されます。ジョブ→ジョブ履歴サブタブ

を開いてみてください。過去に行ったジョブの履歴が一覧になっています。

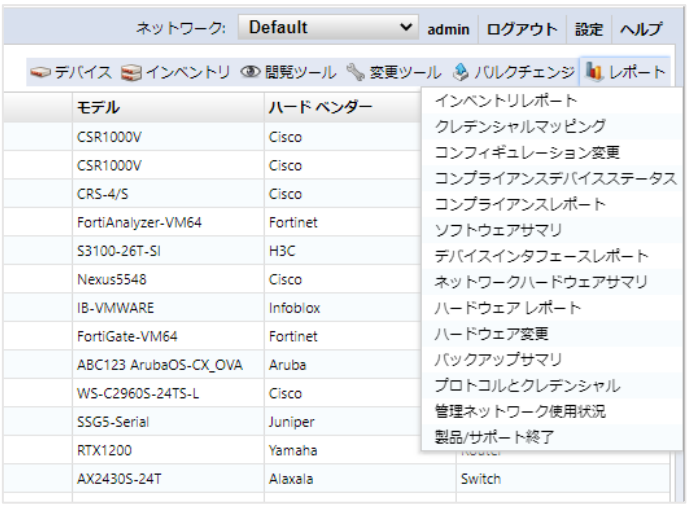
ジョブの完了ステータスは左端のアイコンで示され、以下のような意味をもっています。

アイコン	説明
	全てのデバイスに正常に接続できました。
	一部のデバイスで処理が失敗しました。
	全てのデバイスで処理が失敗しました。

ジョブ履歴をどれほどの期間保存するかの設定方法は、9.5.1 データ保存期間を参照してください。

6.11 レポートの概要

netLD は複数のタイプの読みやすくわかりやすい印刷用統計レポートを出力することが出来ます。メニューから直接出力することも、スケジュール化して出力を自動化することも可能です。レポートツールはレポートサブメニューから実行可能です。

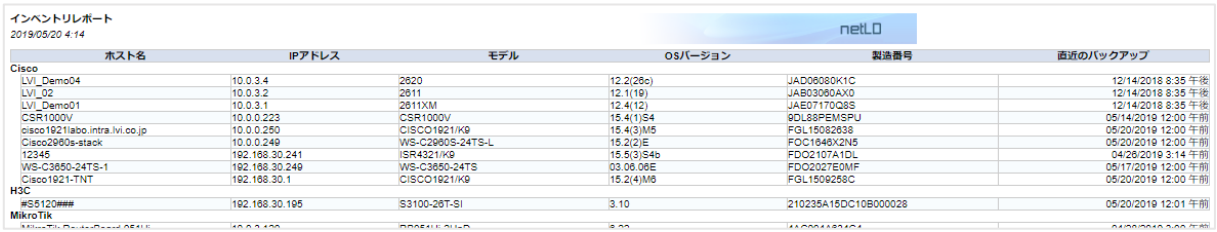


6.11.1 レポートの種類

netLD では、以下の 14 種類の形式でレポートを出力することができます。

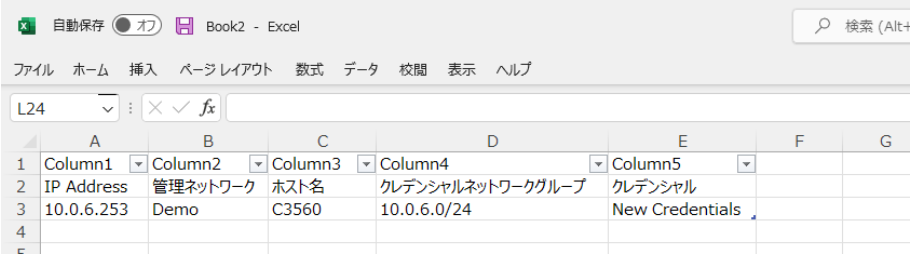
6.11.1.1 インベントリレポート

デバイスのホスト名、IP アドレス、モデル、OS バージョン、シリアル番号、直近バックアップの実行日時をレポート出力します。



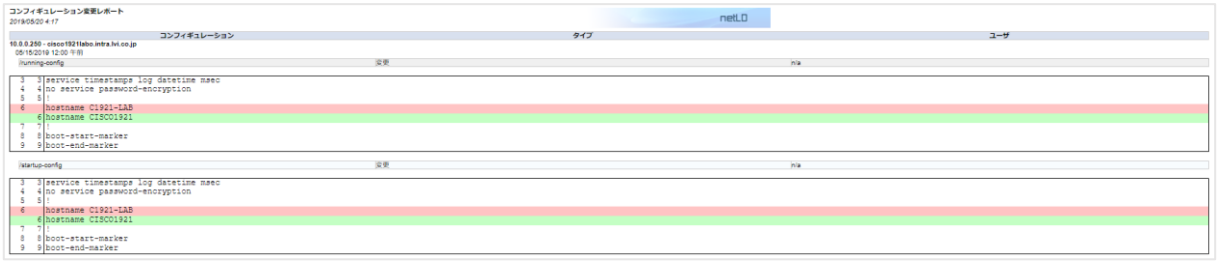
6.11.1.2 クレデンシャルマッピング

デバイスに使用されたクレデンシャルの概要情報を出力します。



6.11.1.3 コンフィギュレーション変更

指定期間内に変更されたコンフィギュレーションの更新履歴と内容をレポート出力します。


コンフィギュレーション変更レポート
2019/05/20 4:17
netLO

コンフィギュレーション	タイプ	ユーザ
10.0.0.250 - cisco1921labo.intra.lvi.co.jp 05/15/2019 12:00 午前		
/running-config	変更	n/a

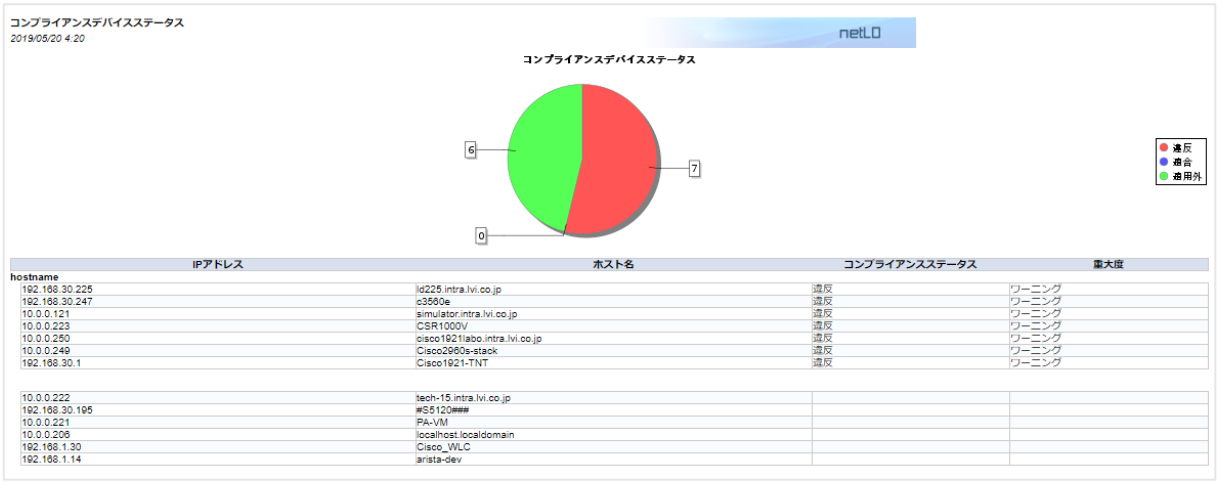
```
3  3 service timestamps log datetime msec
4  4 no service password-encryption
5  5 !
6    hostname C1921-LAB
   6 hostname CISCO1921
7  7 !
8  8 boot-start-marker
9  9 boot-end-marker
```

/startup-config	変更	n/a

```
3  3 service timestamps log datetime msec
4  4 no service password-encryption
5  5 !
6    hostname C1921-LAB
   6 hostname CISCO1921
7  7 !
8  8 boot-start-marker
9  9 boot-end-marker
```

6.11.1.4 コンプライアンスデバイスステータス

現在のコンプライアンスの内容と適用状況をポリシー単位で出力します。


コンプライアンスデバイスステータス
2019/05/20 4:20
netLO

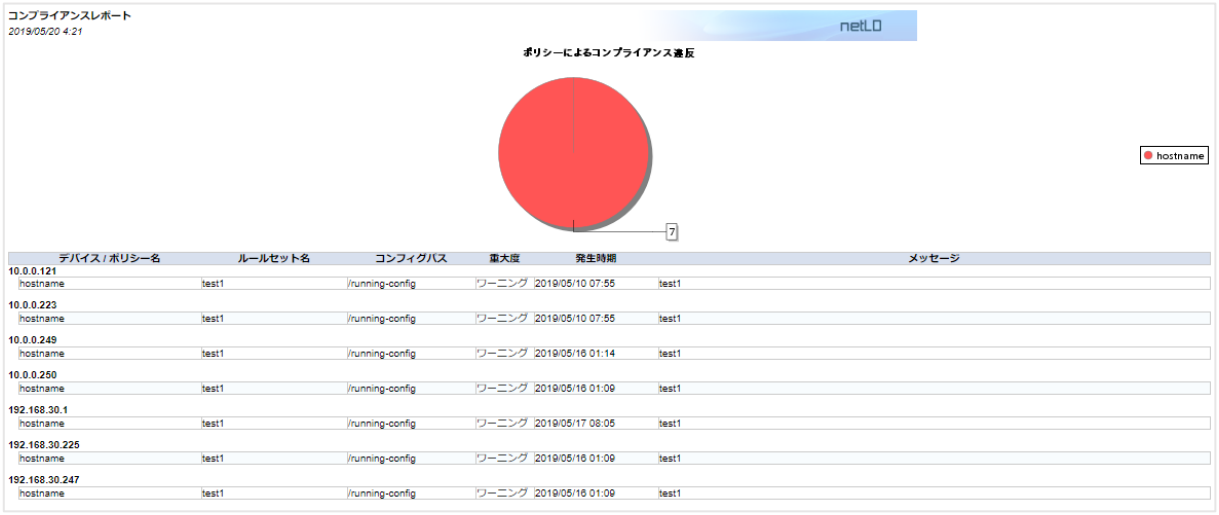
コンプライアンスデバイスステータス

違反
適合
適用外

IPアドレス	ホスト名	コンプライアンスステータス	重大度
hostname			
192.168.30.225	id225.intra.lvi.co.jp	違反	ワーニング
192.168.30.247	c3560e	違反	ワーニング
10.0.0.121	sinnulator.intra.lvi.co.jp	違反	ワーニング
10.0.0.223	CSR1000V	違反	ワーニング
10.0.0.250	cisco1921labo.intra.lvi.co.jp	違反	ワーニング
10.0.0.249	Cisco2960s-stack	違反	ワーニング
192.168.30.1	Cisco1921-TNT	違反	ワーニング
10.0.0.222	tech-15.intra.lvi.co.jp		
192.168.30.195	#5120###		
10.0.0.221	PA-VM		
10.0.0.206	localhost.localdomain		
192.168.1.30	Cisco_WLC		
192.168.1.14	arista-dev		

6.11.1.5 コンプライアンスレポート

現在コンプライアンス違反している内容をデバイスごとに出力します。


コンプライアンスレポート
2019/05/20 4:21
netLO

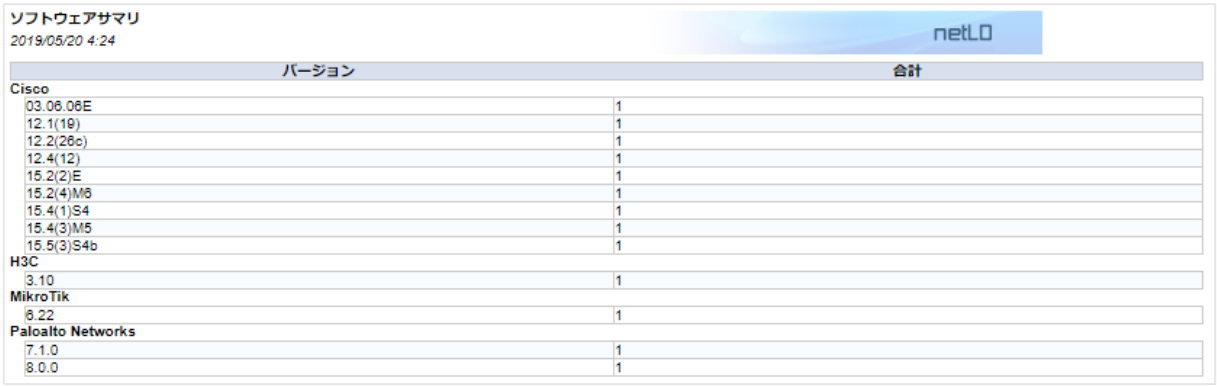
ポリシーによるコンプライアンス違反

hostname

デバイス / ポリシー名	ルールセット名	コンフィグパス	重大度	発生時期	メッセージ
10.0.0.121					
hostname	test1	/running-config	ワーニング	2019/05/10 07:55	test1
10.0.0.223					
hostname	test1	/running-config	ワーニング	2019/05/10 07:55	test1
10.0.0.249					
hostname	test1	/running-config	ワーニング	2019/05/16 01:14	test1
10.0.0.250					
hostname	test1	/running-config	ワーニング	2019/05/16 01:09	test1
192.168.30.1					
hostname	test1	/running-config	ワーニング	2019/05/17 08:05	test1
192.168.30.225					
hostname	test1	/running-config	ワーニング	2019/05/16 01:09	test1
192.168.30.247					
hostname	test1	/running-config	ワーニング	2019/05/16 01:09	test1

6.11.1.6 ソフトウエアサマリ

デバイスで動作している OS のサマリレポートを出力します。

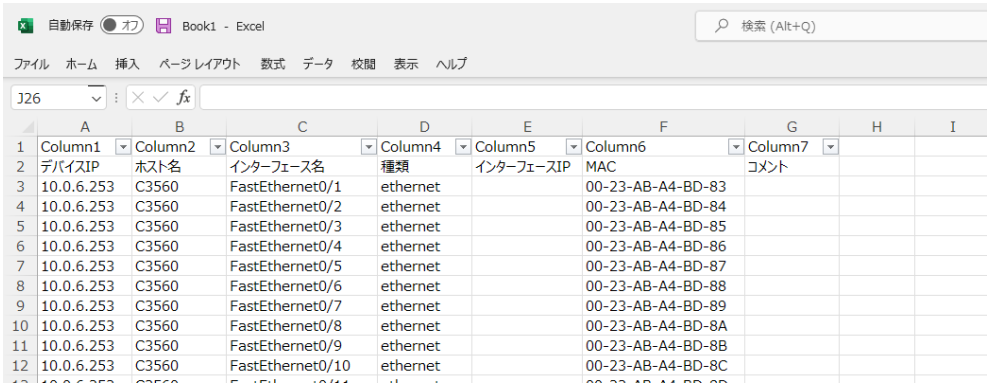


ソフトウェアサマリ
2019/05/20 4:24
netLD

バージョン	合計
Cisco	
03.06.06E	1
12.1(19)	1
12.2(26c)	1
12.4(12)	1
15.2(2)E	1
15.2(4)M6	1
15.4(1)S4	1
15.4(3)M5	1
15.5(3)S4b	1
H3C	
3.10	1
MikroTik	
6.22	1
Paloalto Networks	
7.1.0	1
8.0.0	1

6.11.1.7 デバイスインタフェースレポート

デバイスのインタフェースの情報を出力します。



自動保存 オフ Book1 - Excel 検索 (Alt+Q)

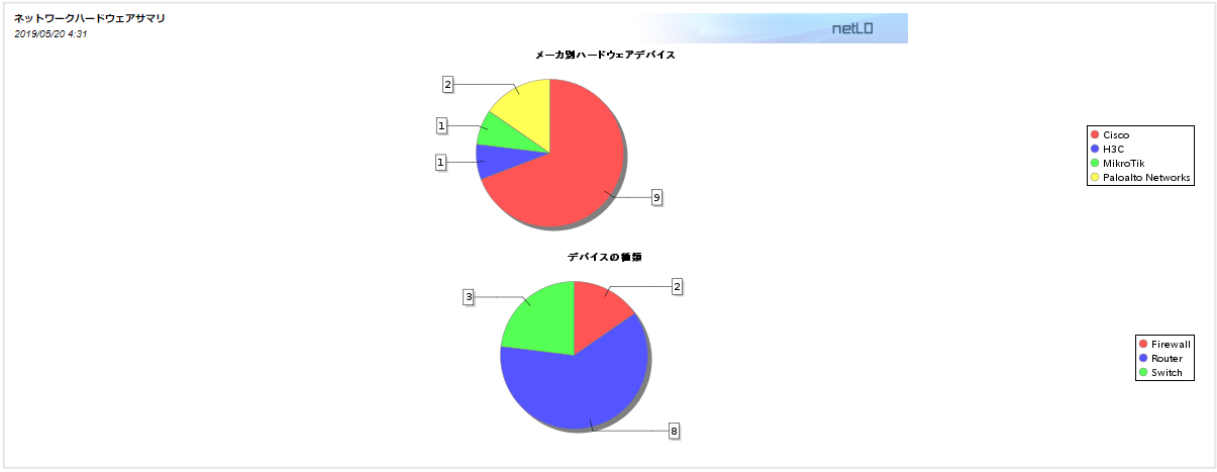
ファイル ホーム 挿入 ページ レイアウト 数式 データ 校閲 表示 ヘルプ

J26

	A	B	C	D	E	F	G	H	I
1	Column1	Column2	Column3	Column4	Column5	Column6	Column7		
2	デバイスIP	ホスト名	インターフェース名	種類	インターフェースIP	MAC	コメント		
3	10.0.6.253	C3560	FastEthernet0/1	ethernet		00-23-AB-A4-BD-83			
4	10.0.6.253	C3560	FastEthernet0/2	ethernet		00-23-AB-A4-BD-84			
5	10.0.6.253	C3560	FastEthernet0/3	ethernet		00-23-AB-A4-BD-85			
6	10.0.6.253	C3560	FastEthernet0/4	ethernet		00-23-AB-A4-BD-86			
7	10.0.6.253	C3560	FastEthernet0/5	ethernet		00-23-AB-A4-BD-87			
8	10.0.6.253	C3560	FastEthernet0/6	ethernet		00-23-AB-A4-BD-88			
9	10.0.6.253	C3560	FastEthernet0/7	ethernet		00-23-AB-A4-BD-89			
10	10.0.6.253	C3560	FastEthernet0/8	ethernet		00-23-AB-A4-BD-8A			
11	10.0.6.253	C3560	FastEthernet0/9	ethernet		00-23-AB-A4-BD-8B			
12	10.0.6.253	C3560	FastEthernet0/10	ethernet		00-23-AB-A4-BD-8C			

6.11.1.8 ネットワークハードウェアサマリ

メーカ、デバイスの種類の円グラフをレポート出力します。



6.11.1.9 ハードウェアレポート

ハードウェア情報（筐体、カード、パワーサプライのモデル名、シリアル、説明、スロットタイプ、FRU 等）をレポート出力します。サポート契約の精査に役立ちます。

ハードウェア レポート

2019/05/20 4:32

タイプ	スロット番号	スロットタイプ	モデル	製造番号	シリアル番号	説明
10.0.0.221 - PA-VM - Firewall						
Chassis			PA-VM		unknown	Paloalto Firewall
10.0.0.222 - tech-15.intra.lvi.co.jp - Firewall						
Chassis			PA-VM		unknown	Paloalto Firewall
10.0.0.223 - CSR1000V - Router						
Chassis			CSR1000V		9DL88PEMSPU	Cisco CSR1000V Chassis
10.0.0.249 - Cisco2960s-stack - Switch						
Chassis			WS-C2960S-24TS-L		FOC1721W1SR	WS-C2960S-24TS-L
Chassis			WS-C2960S-24TS-L		FOC1646X2N5	WS-C2960S-24TS-L
Card	1	Stack	WS-C2960S-24TS-L	73-11910-08	FOC16456SF8	Master Switch
PowerSuppl			WS-C2960S-24TS-L	341-0328-02	DCA1641MGKH	Power Supply
Chassis						
Card	2	Stack	WS-C2960S-24TS-L	73-11910-09	FOC17211A22	Member Switch
PowerSuppl			WS-C2960S-24TS-L	341-0328-02	DCA1716M7B2	Power Supply
10.0.0.250 - cisco1921labo.intra.lvi.co.jp - Router						
Chassis			CISCO1921/K9		FGL15082638	CISCO1921/K9 chassis, Hw Serial#: FGL15082638, Hw Revision: 1.0
Card	0	physical	CISCO1921/K9	73-12850-03	FOC15052D7A	C1921 Mother board 2GE, integrated VPN and 2W Port adapter, 2 ports
10.0.3.1 - LVI_Demo01 - Router						
Chassis			CISCO2611XM-2FE		JAE07170Q8S	2611XM chassis
Card	0	physical	C2611XM-2FE	73-7679-02	FFFF	C2611XM 2FE Mainboard Port adapter, 2 ports

6.11.1.10 ハードウェア変更

指定期間内に変更されたハードウェアの変更履歴と内容をレポート出力します。

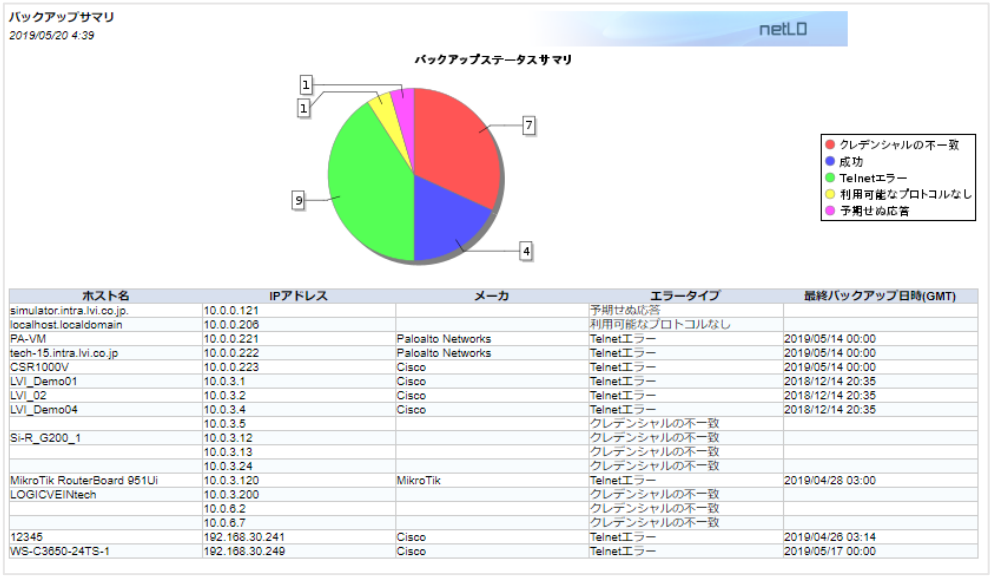
ハードウェア変更レポート

2019/05/20 4:38

タイプ	スロット番号	スロットタイプ	モデル	製造番号	シリアル番号	説明
10.0.0.249 - Cisco2960s-stack - Switch						
05/08/2019 3:00 午前						
Chassis			WS-C2960S-24TS-L		FOC1646X2N5	WS-C2960S-24TS-L
Chassis			WS-C2960S-24TS-L		FOC1721W1SR	WS-C2960S-24TS-L
Chassis						
Card	1	Stack	WS-C2960S-24TS-L	73-11910-08	FOC16456SF8	Master Switch
Card	2	Stack	WS-C2960S-24TS-L	73-11910-09	FOC17211A22	Member Switch
PowerSuppl			WS-C2960S-24TS-L	341-0328-02	DCA1641MGKH	Power Supply
PowerSuppl			WS-C2960S-24TS-L	341-0328-02	DCA1716M7B2	Power Supply
192.168.30.1 - Cisco1921-TNT - Router						
05/17/2019 7:59 午前						
Chassis			CISCO1921/K9		FGL1509258C	CISCO1921/K9 chassis, Hw Serial#: FGL1509258C, Hw Revision: 1.0
Card	0	physical	CISCO1921/K9	73-12850-03	FOC15073NYY	C1921 Mother board 2GE, integrated VPN and 2W Port adapter, 3 ports
Daughter	0	physical	EHWIC-1GE-SFP-CU	73-13295-01	FOC15400RGF	1 Port Gigabit Ethernet SFP/Copper EHWIC
192.168.30.195 - #S5120### - Switch						
05/08/2019 8:13 午前						
Chassis			S3100-26T-SI		210235A15DC10B000028	H3C S3100-26T-SI

6.11.1.11 バックアップサマリ

バックアップに成功/失敗したデバイスの統計情報や失敗理由の簡易情報をレポート出力します。



バックアップサマリ

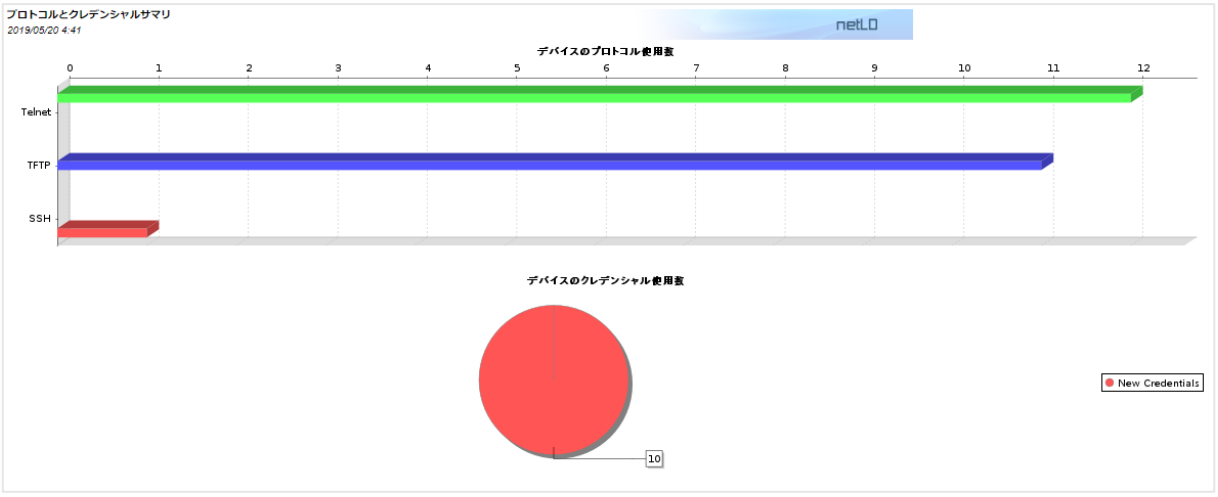
2019/05/20 4:39

バックアップステータスサマリ

ホスト名	IPアドレス	メーカ	エラータイプ	最終バックアップ日時(GMT)
simulator.intra.lvi.co.jp.	10.0.0.121		予期せぬ応答	
localhost.localdomain	10.0.0.206		利用可能なプロトコルなし	
PA-VM	10.0.0.221	Paloalto Networks	Telnetエラー	2019/05/14 00:00
tech-15.intra.lvi.co.jp	10.0.0.222	Paloalto Networks	Telnetエラー	2019/05/14 00:00
CSR1000V	10.0.0.223	Cisco	Telnetエラー	2019/05/14 00:00
LVI_Demo01	10.0.3.1	Cisco	Telnetエラー	2018/12/14 20:35
LVI_02	10.0.3.2	Cisco	Telnetエラー	2018/12/14 20:35
LVI_Demo04	10.0.3.4	Cisco	Telnetエラー	2018/12/14 20:35
	10.0.3.5		クレデンシャルの不一致	
Si-R_G200_1	10.0.3.12		クレデンシャルの不一致	
	10.0.3.13		クレデンシャルの不一致	
	10.0.3.24		クレデンシャルの不一致	
MikroTik RouterBoard 951Ui	10.0.3.120	MikroTik	Telnetエラー	2019/04/28 03:00
LOGICVEINtech	10.0.3.200		クレデンシャルの不一致	
	10.0.6.2		クレデンシャルの不一致	
	10.0.6.7		クレデンシャルの不一致	
12345	192.168.30.241	Cisco	Telnetエラー	2019/04/26 03:14
WS-C3650-24TS-1	192.168.30.249	Cisco	Telnetエラー	2019/05/17 00:00

6.11.1.12　プロトコルとクレデンシャル

使用されたプロトコルとクレデンシャルのサマリをレポート出力します。



6.11.1.13　管理ネットワーク使用状況

ユーザが管理しているネットワークに登録されているデバイス数をレポート出力します。

管理ネットワーク使用状況
2019/05/28 6:50
netLD

管理ネットワーク	スマートブリッジ	デバイス数
Default	Default	16
LogicVein	Default	0
test	Default	0
	合計デバイス数	16

6.11.1.14　製品/サポート終了

デバイスの製品終了・サポート終了日をレポート出力します。

End Of Sale/End Of Life Report
2022年10月12日 18:44

ホスト名	IPアドレス	メーカ	モデル	OSバージョン	デバイスタイプ	製造番号	製品終了	サポート終了
CR3-A	10.0.0.121	Cisco	CRS-4/S	4.3.1	Router	SMA112502OL	08/15/2014	08/31/2021
Demo20201222	10.0.0.249	Cisco	WS-C2960S-24TS-L	15.2(2)E	Switch	FOC1646X2N5	11/08/2015	11/30/2020
NER3-LVI	10.128.0.1	Cisco	CRS-16/S	4.2.1	Router	TBA10340015	07/31/2013	07/31/2020
	10.128.0.6	Cisco	CRS-4/S	4.3.1	Router	SMA112502OL	08/15/2014	08/31/2021
simulator	10.128.0.7	Cisco	CRS-8/S	4.3.1	Router	TBA09500081	07/31/2013	07/31/2020
simulator	10.128.0.8	Cisco	CRS-8/S	4.3.1	Router	TBA09500075	07/31/2013	07/31/2020
CR4-B	10.128.0.9	Cisco	CRS-4/S	4.3.1	Router	SMA112502OH	08/15/2014	08/31/2021
CR3-A	10.128.0.10	Cisco	CRS-4/S	4.3.1	Router	SMA112502OL	08/15/2014	08/31/2021
NER4-B	10.128.0.11	Cisco	CRS-16/S	4.2.1	Router	TBA10380117	07/31/2013	07/31/2020
NER5-A	10.128.0.12	Cisco	CRS-4/S	4.3.1	Router	SMA124506YQ	08/15/2014	08/31/2021
CR7-A	10.128.0.13	Cisco	CRS-4/S	4.3.1	Router	SMA1236098P	08/15/2014	08/31/2021
CR8-B	10.128.0.14	Cisco	CRS-4/S	4.3.1	Router	SMA1236098O	08/15/2014	08/31/2021
NER5-A	10.128.0.15	Cisco	CRS-4/S	4.3.1	Router	SMA124506YQ	08/15/2014	08/31/2021
NER6-B	10.128.0.16	Cisco	CRS-4/S	4.3.1	Router	SMA1246077Z	08/15/2014	08/31/2021
CR5-A	10.128.0.17	Cisco	CRS-16/S	4.3.1	Router	TBM14481618	07/31/2013	07/31/2020
CR9-A	10.128.0.21	Cisco	CRS-4/S	4.3.1	Router	SMA124506WH	08/15/2014	08/31/2021
CR1-A	10.128.0.22	Cisco	CRS-16/S	4.3.1	Router	TBA09520157	07/31/2013	07/31/2020
CR2-B	10.128.0.23	Cisco	CRS-16/S	4.3.1	Router	TBA09520158	07/31/2013	07/31/2020
NER3-A	10.128.0.24	Cisco	CRS-16/S	4.2.1	Router	TBA10340015	07/31/2013	07/31/2020
NER5-A	10.128.0.26	Cisco	CRS-4/S	4.3.1	Router	SMA124506YQ	08/15/2014	08/31/2021
SCE8000	10.128.0.76	Cisco	SCE8000	3.7.2-p3 Build 352	Content Engine	FOX1414GAXK	10/01/2015	09/30/2020
CR8-B	10.128.0.98	Cisco	CRS-4/S	4.3.1	Router	SMA1236098O	08/15/2014	08/31/2021
CR8-B	10.128.0.99	Cisco	CRS-4/S	4.3.1	Router	SMA1236098O	08/15/2014	08/31/2021

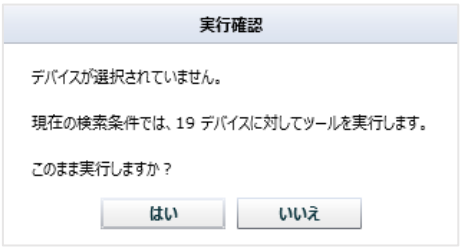
6.11.2　手動でレポート通常発行

レポートを閲覧したい時に手動で出力します。上で挙げた 14 のレポートには、2 つのタイプがあります。基本的には、レポート発行したいデバイスを選択し発行することでレポートは生成されますが、レポートによっては、同じネットワーク内に登録されている全ての機器が対象となるレポートがあります。

インベントリ全体に対して行われるレポート	ネットワークハードウェアサマリ
	コンプライアンスデバイスステータス
	管理ネットワーク使用状況
	製品/サポート終了
デバイスごとに生成できるレポート	インベントリレポート
	クレデンシャルマッピング
	コンフィギュレーション変更
	コンプライアンスレポート
	ソフトウェアサマリ
	デバイスインタフェースレポート
	ハードウェア レポート
	ハードウェア変更
	バックアップサマリ
	プロトコルとクレデンシャル

ここでは、インベントリレポートの作成を試してみます。レポートに含めたいデバイスをデバイスビューで選択しておいてください。全デバイスを対象にする場合には、何も選択せず実行してください。

デバイスを選択せずに表の右側のレポートを実行すると、以下の確認ダイアログが現れます。デバイスの数がとても多い場合には、コンピュータがハングアップしてしまう可能性があるので気をつけてください。

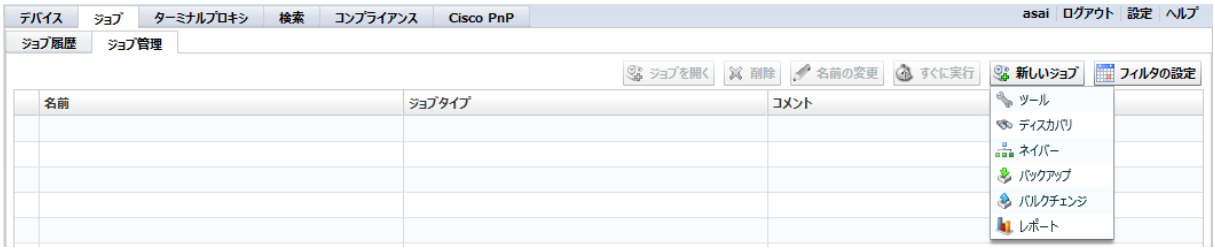


レポート形式を選択して OK ボタンを押してください。

レポートに記載される情報はバックアップ時の情報を使用しております。最新の情報をレポートに反映させたい場合には、必ずバックアップ後にレポートを発行してください。

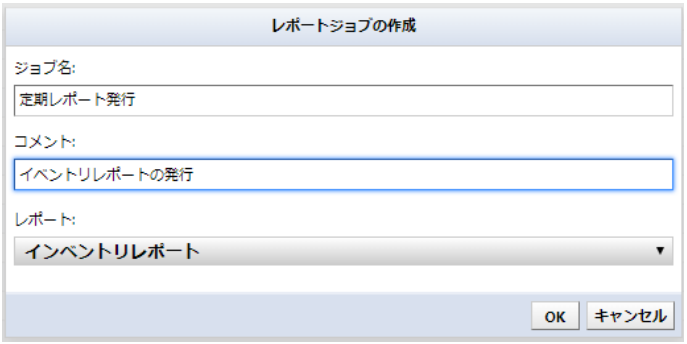
6.11.3　レポートの定期発行

レポートを定期発行し、さらに運用管理者へメールで送信することが可能です。この設定はジョブ機能を使用します。以下の手順はインベントリレポートを例にしています。レポートの定期発行は、ジョブタブ→新しいジョブ→レポートから行います。ジョブの作成は「ジョブ管理」でも説明しておりますが、以下では、インベントリレポートの発行を説明します。このレポート・ジョブも、基本的なジョブ作成の流れに則っています。



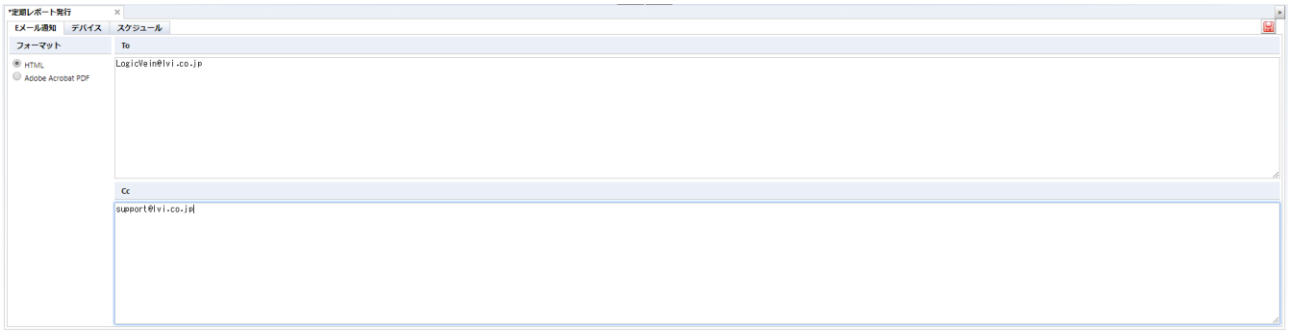
ジョブ名前を決め、使う機能を選びます。

ジョブの名前とコメントを入力し、レポートタイプをリストから選びます。今回はインベントリレポートです。終わったら、OK ボタンを押してください。



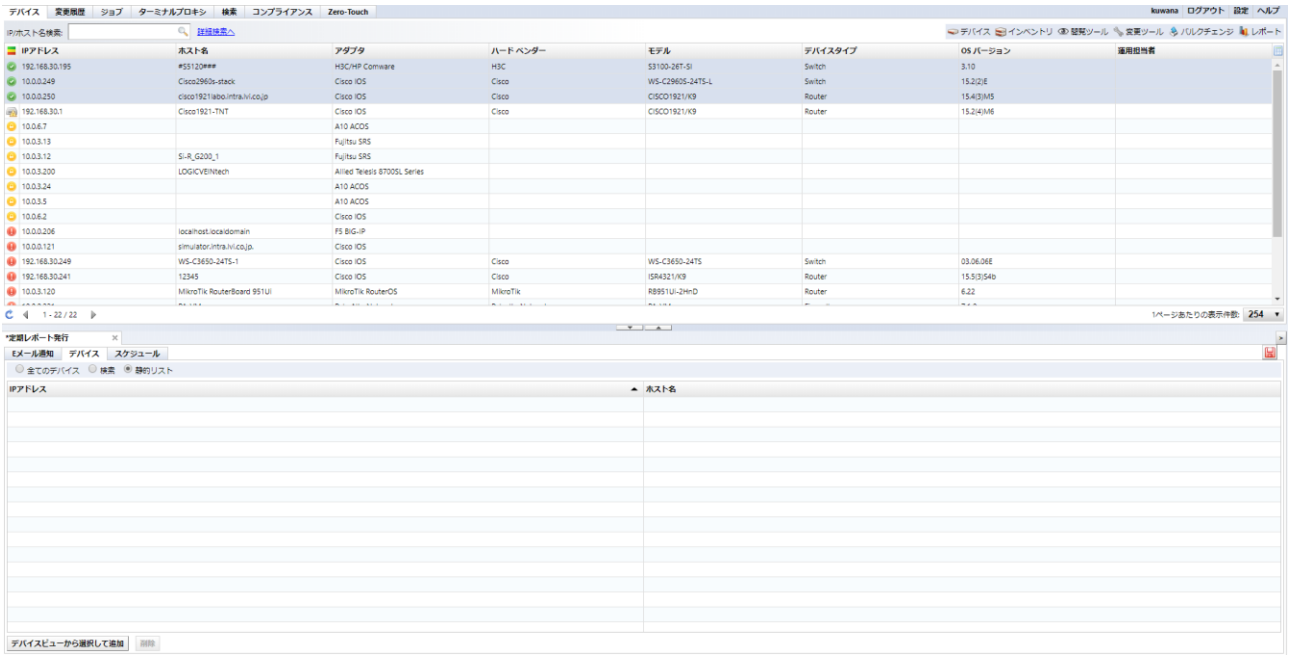
必要なパラメータを入力します。

ステータスペインに新しいタブが現れます。E メール通知サブタブで、レポートフォーマットを HTML か PDF かで選んでください。メールの受信者を To,Cc に入力します。ただし、メール受信のためには SMTP サーバをセットアップする必要があります。詳細は「メールサーバ機能」をご覧ください。



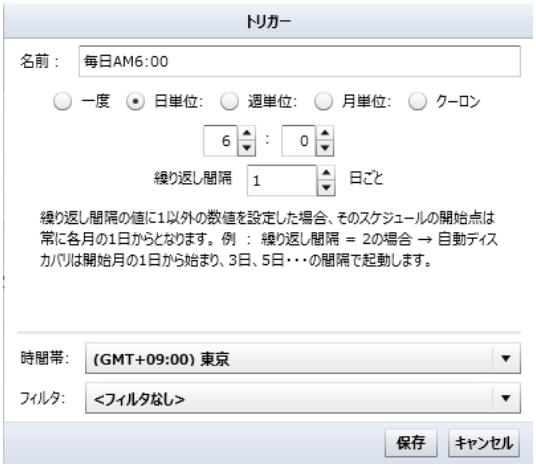
対象デバイスを選びます。

デバイスビューからデバイスをステータスペインのデバイスサブタブに追加します。



ジョブのトリガー(実行頻度)を入力します。

トリガーを設け、レポート発行の頻度を設定します。

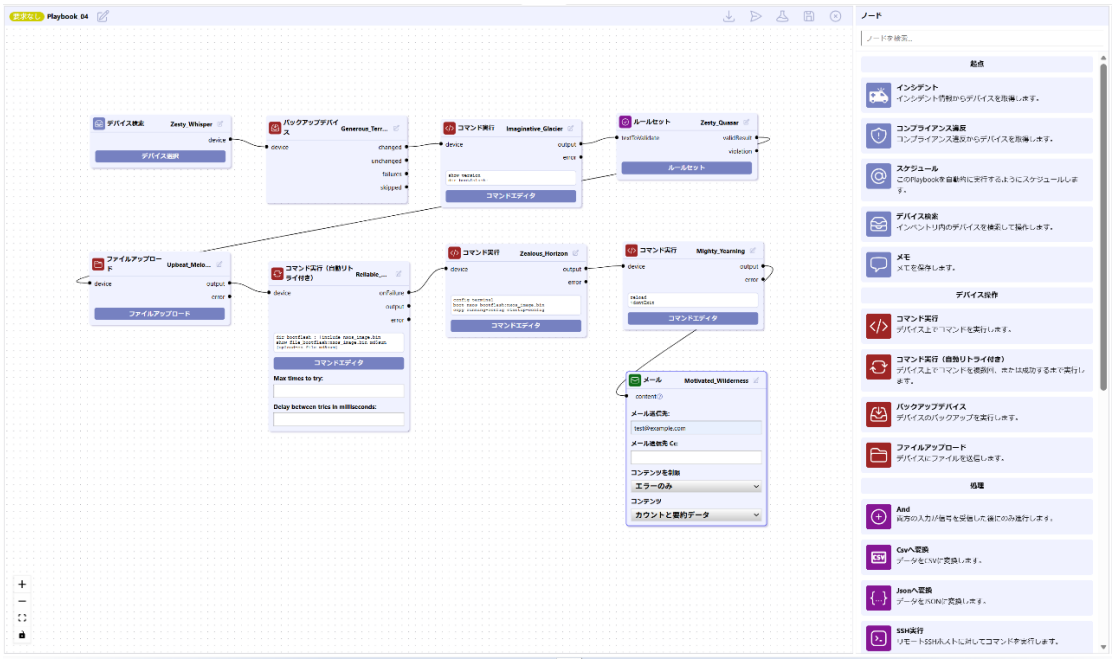


最後に  を押してジョブを保存することを忘れないようにしてください。一旦設定すれば、レポートはメールで自動的に送られるようになります。

6.12 Playbook

6.12.1 Playbook の概要

Playbook 機能は、複数のジョブやコマンドの実行結果を組み合わせて、一連のタスクを自動化できる機能です。従来のジョブ機能は、show コマンドなどを実行する一方向の処理フローで完結します。一方、Playbook では、show コマンド実行後、その結果に基づいて条件分岐して、追加のコマンドを実行したり、メール通知を送信したりすることができます。これによって、より複雑な業務フローを自動化し、効率的な運用を実現できます。



6.12.2 Playbook ノード

Playbook では、アクションを表す「ノード」と呼ばれるボックスを線でつなげて、一連のタスクを構築します。ノードは機能別に 4 つのカテゴリに大別されます。カテゴリごとのノードの種類とその説明を、次の表に示します。

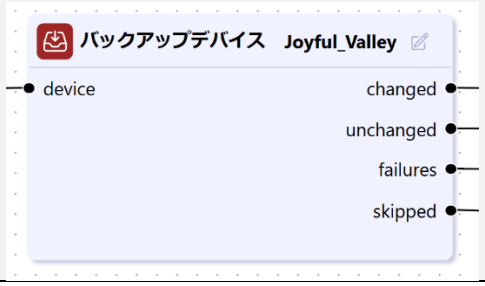
1．「起点」ノード：Playbook にデバイスを追加し、プロセスを開始するノードです。

ノードアイコン	ノードラベル	説明
	コンプライアンス違反	コンプライアンス違反が発生したデバイスに関する情報を次のノードに送信します。 

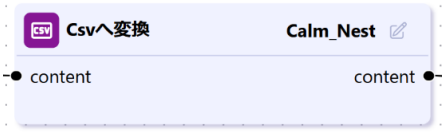
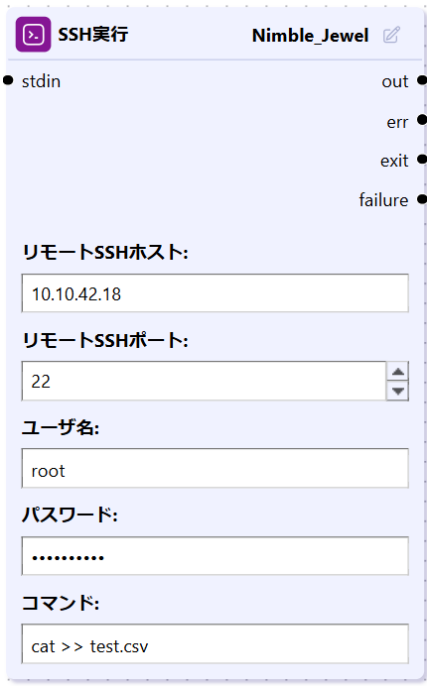
ノードアイコン	ノードラベル	説明
	スケジュール	Playbook を自動的に実行するようにスケジュールします。このノードは次のノードに接続されていなくても、有効に設定されていれば実行されます。 
	デバイス検索	Playbook 開始時に、検索条件に一致したデバイスに関する情報を次のノードに送信します。検索方法には、「全てのデバイス」、「検索」、「静的リスト」の 3 つがあります。 
	メモ	Playbook 画面にメモを保存します。一連のタスクにメモを追加し、その内容を次のノードに送信できます。また、このメモは Playbook の内容を把握する際にも役立ちます。 

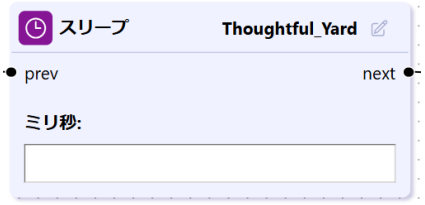
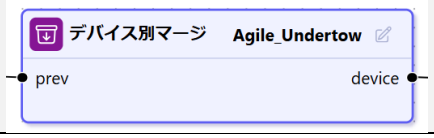
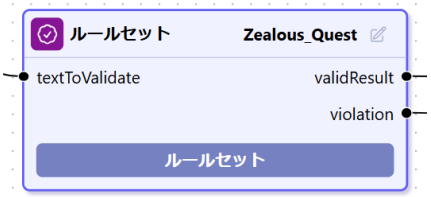
2. 「デバイス操作」ノード：CLI コマンドを送信し、デバイスを操作するノードです。

ノードアイコン	ノードラベル	説明
	コマンド実行	前のノードから受信した対象デバイスの情報をもとに、指定されたコマンドを実行し、その結果を次のノードに送信します。 

ノードアイコン	ノードラベル	説明
	コマンド実行 （自動リトライ付き）	前のノードから受信した対象デバイスの情報をもとに、指定されたコマンドを、指定回数実行します。リトライは、「Delay between tries in milliseconds:」で指定されたミリ秒間隔で、指定された回数行われます。 
	バックアップデバイス	デバイスのバックアップを実行し、バックアップの結果（「変更あり」、「変更なし」、「失敗」、「スキップ」）に基づいて処理を分岐します。 
	ファイルアップロード	前のノードから受信した対象デバイスにファイルを送信します。サポートされているプロトコルは、FTP/TFTP/SCP です。 

3. 「処理」ノード：データ処理や条件分岐・制御を行うノードです。

ノードアイコン	ノードラベル	説明
	And	a と b の両方の入力信号が受信された後、処理が進行します。各入力から受信した情報は、ノードの右側にある a と b それぞれから次のノードに送信されます。 
	Csv へ変換	出力されたデータを Csv フォーマットへ変換します。 
	Json へ変換	出力されたデータを Json フォーマットへ変換します。 
	SSH 実行	データを受信した後に SSH ホストに対してコマンドを実行し、結果を次のノードに送信します。 

ノードアイコン	ノードラベル	説明
	コンフィグ読み込み	最新のバックアップコンフィギュレーションを読み込みます。 
	スリープ	指定されたミリ秒数だけ、入力の送信を遅延させます。 
	デバイス別マージ	デバイスごとに出力を一つにまとめます。 
	ルールセット	前のノードから受信したコマンドの実行結果などのテキストデータを、指定されたルールセットに従って評価し、その結果を次のノードに送信します。 
	正規表現一致	前のノードから受信したコマンドの出力結果に対して、正規表現を用いた文字列検索を実行します。検索結果が正規表現にマッチしたかどうかに応じて、処理を分岐させることができます。また、「Partial Match」オプションを有効にすることで、部分一致の検索も可能です。 

ノードアイコン	ノードラベル	説明
	変数の設定	変数を設定し、次のノードへ指定した値を送信します。 

4.「出力」ノード：実行結果を外部、またはシステム内へ出力するノードです。

ノードアイコン	ノードラベル	説明
	コンプライアンス違反検出	コンプライアンス違反としてデバイスのステータスを更新します。このノードを使用するとデバイスプロパティのコンプライアンスタブにコンプライアンス違反として登録されます。 
	チャットアプリ(ウェブフック)	前のノードから実行結果を受信後、その内容をウェブフック経由で指定されたチャットアプリに送信します。通知内容はコマンドの結果ではなく、実行結果の要約です。サポートされているチャットアプリは「Microsoft Teams / Slack / Mattermost / WebEx /LINE WORKS/Google Chat」です。 

ノードアイコン	ノードラベル	説明
	フィールドを編集	デバイスのカスタムフィールドを更新します。{中括弧}で囲んだ変数名を記述することで変数を設定することができます。 
	メール	Playbook の実行結果をメールで送信します。メールの内容は、コンテンツおよびコンテンツ制限のプルダウンで変更することができます。 

6.12.3 Playbook の管理

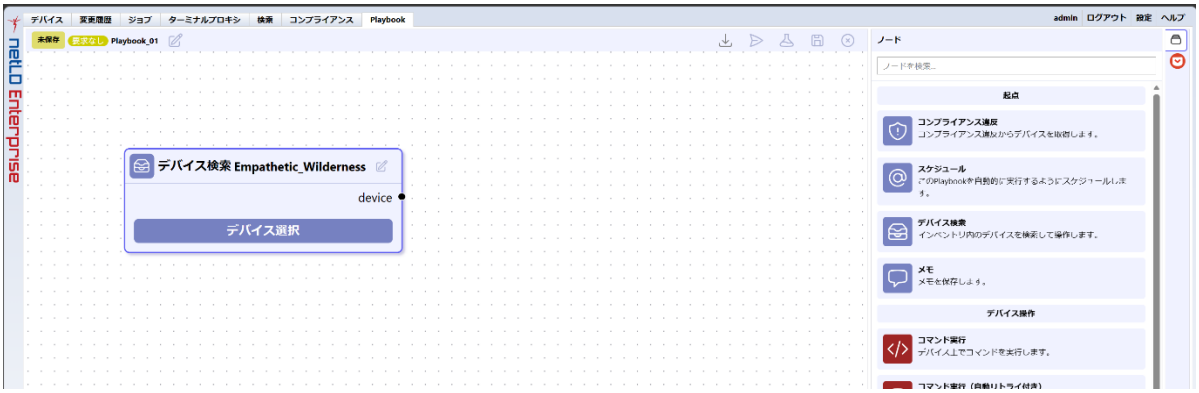
Playbook を管理する方法について説明します。ここでは、新しい Playbook の作成から、既存の Playbook の編集、削除方法について説明します。

6.12.3.1 Playbook の追加

1. ［Playbook］タブを開きます。
2. ［追加］をクリックします。

3. 名前欄に作成する Playbook の名前を入力します。説明欄の入力は任意です。

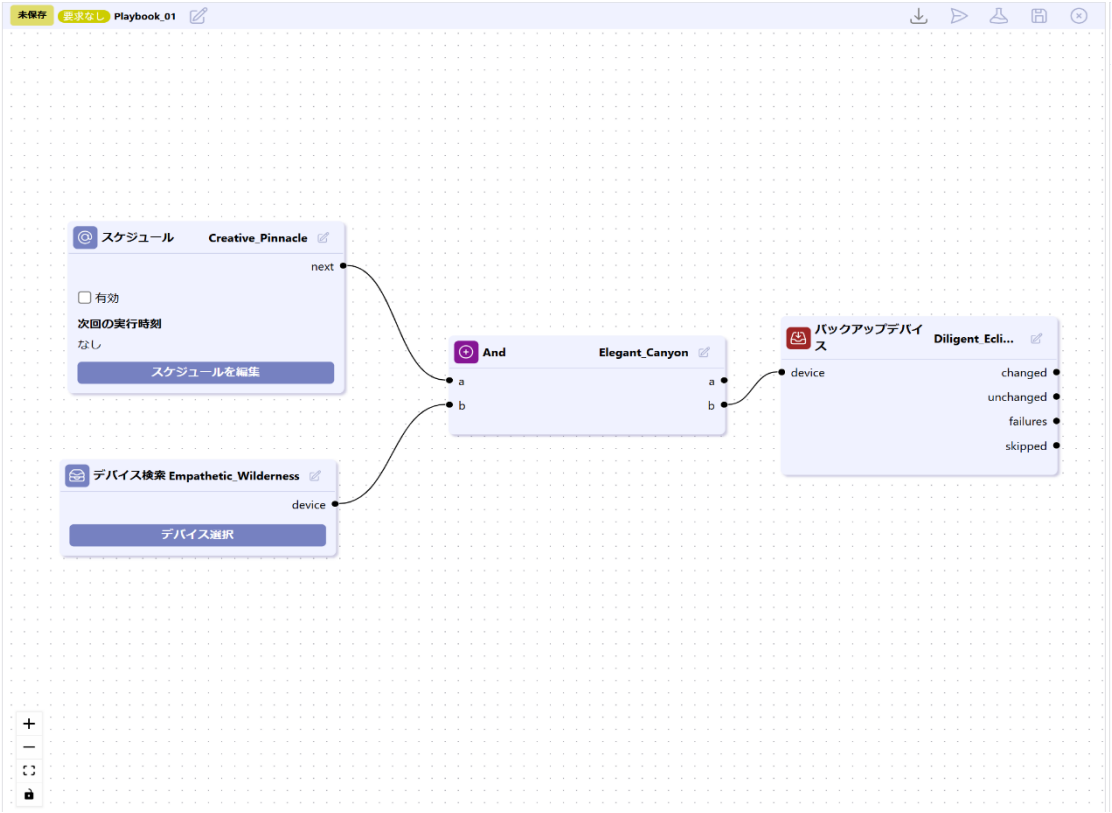
4. ［OK］をクリックします。
5. 画面右側のリストから構成するノードを選択し、左側の表示領域にドラッグ・アンド・ドロップして追加します。



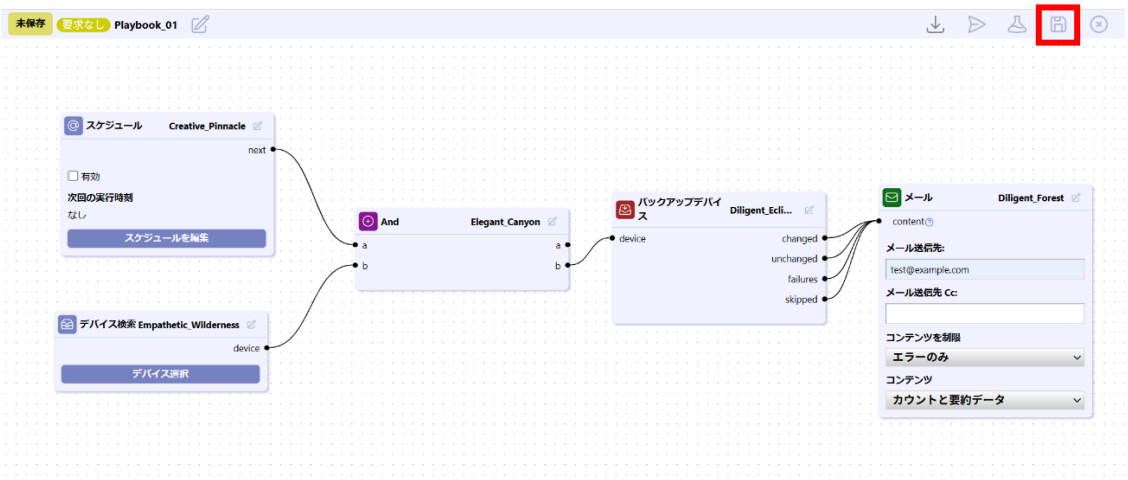
補足

検索ボックスを使用することで、ノード一覧に表示されるノードをノード名で絞り込むことが可能です。

6. ドラッグ操作でノード間を接続します。



7. 編集が完了したら、［Playbook を保存する］ボタンをクリックします。

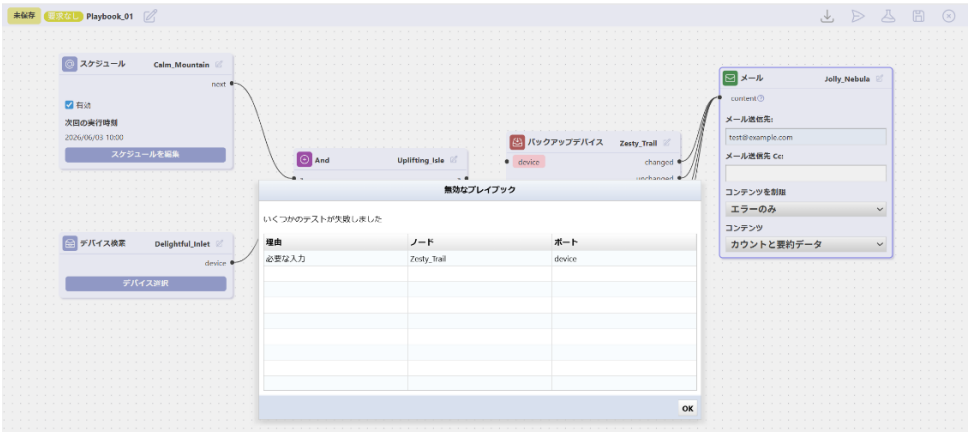


補足

Playbook の設定に無効な設定がないか、以下のアイコンをクリックして確認できます。

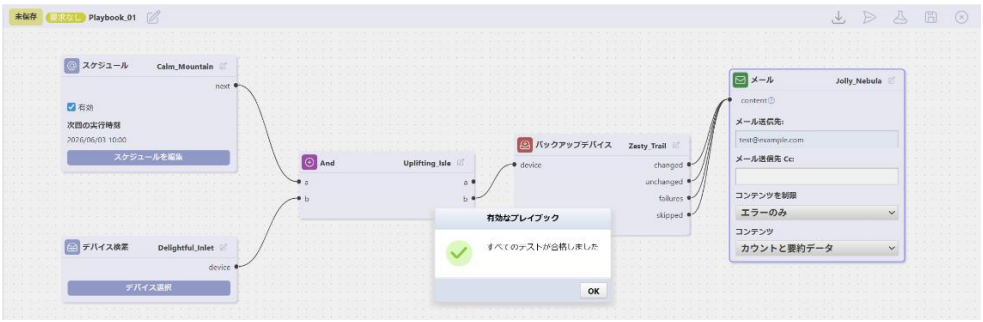
＜無効な設定がある場合＞

無効な設定がある箇所はテーブル形式で表示され、修正が必要な箇所は赤色でハイライトされます。



＜無効な設定がない場合＞

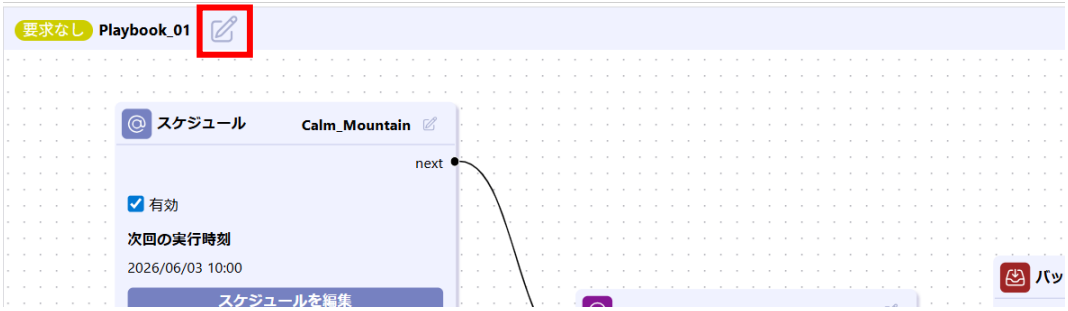
「すべてのテストが合格しました」というメッセージが表示されます。



6.12.3.2 Playbook の編集

1. ［Playbook］タブを開きます。
2. 編集する Playbook を選択してダブルクリックするか、［編集］ボタンをクリックします。

※ ［Playbook の詳細を編集する］をクリックすると、Playbook の名前や説明を編集できます。



3. 編集が完了したら、［Playbook を保存する］ボタンをクリックします。

6.12.3.3 Playbook の削除

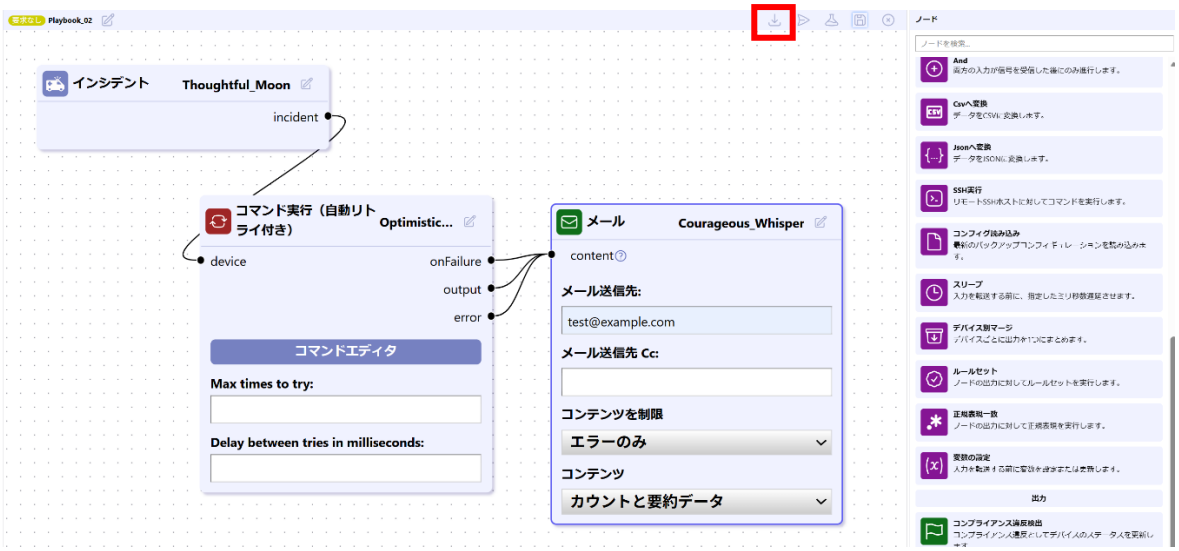
1. ［Playbook］タブを開きます。
2. 削除する Playbook を選択し、［削除］ボタンをクリックします。

3. 確認メッセージが表示されたら、［OK］をクリックします。

4. 一覧から Playbook が削除されます。

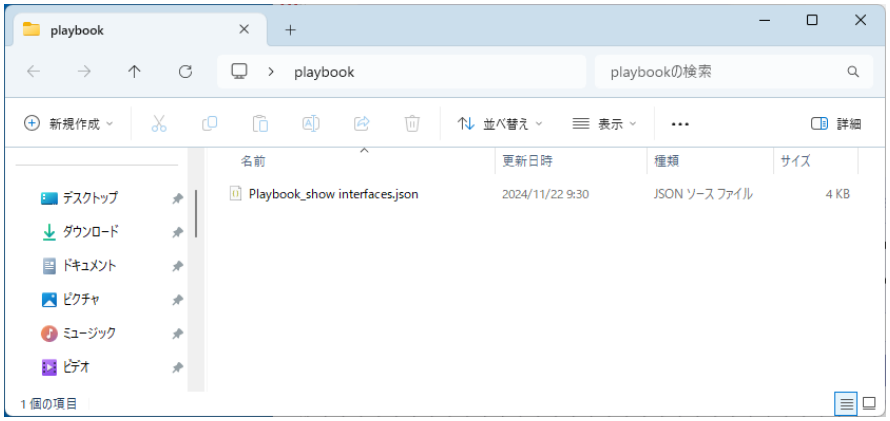
6.12.3.4 Playbook のエクスポート

1. ［Playbook］タブを開きます。
2. エクスポートする Playbook を選択してダブルクリックするか、［編集］ボタンをクリックします。
3. ［Playbook をエクスポート］ボタンをクリックします。



4. ファイルをダウンロードします。

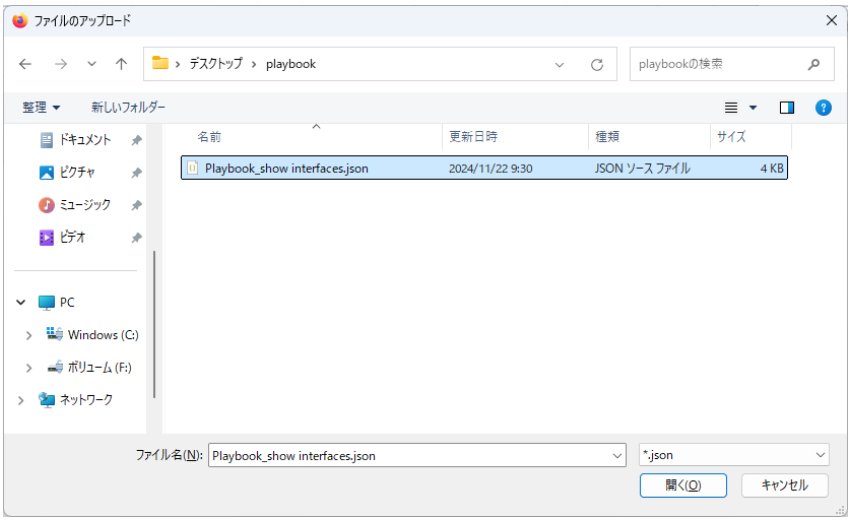
※ ファイルは、JSON ファイル形式で出力されます。



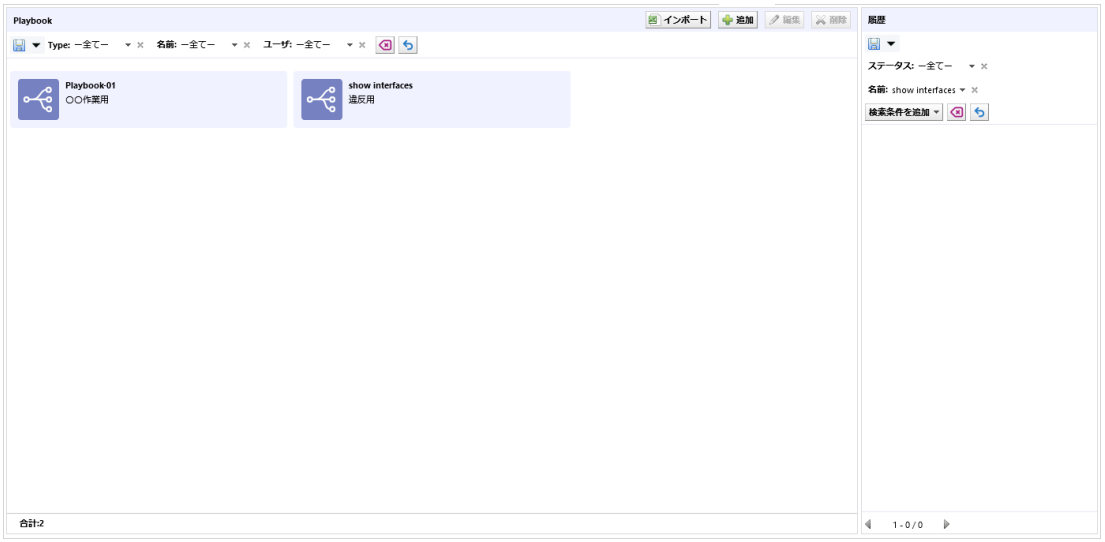
6.12.3.5 Playbook のインポート

1. ［Playbook］タブを開きます。
2. ［インポート］ボタンをクリックします。

3. インポートするファイルを選択し、開きます。



4. インポートが完了すると、一覧に追加されます。



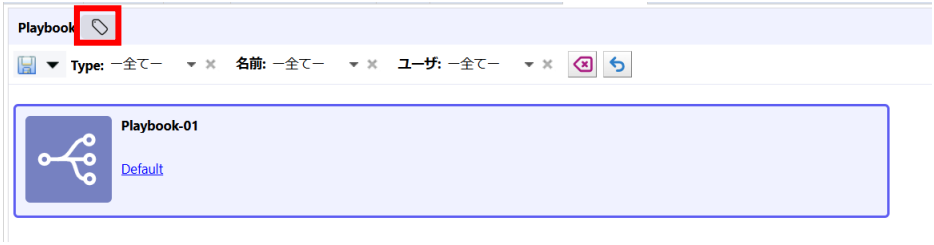
6.12.3.6 Playbook のカテゴリ

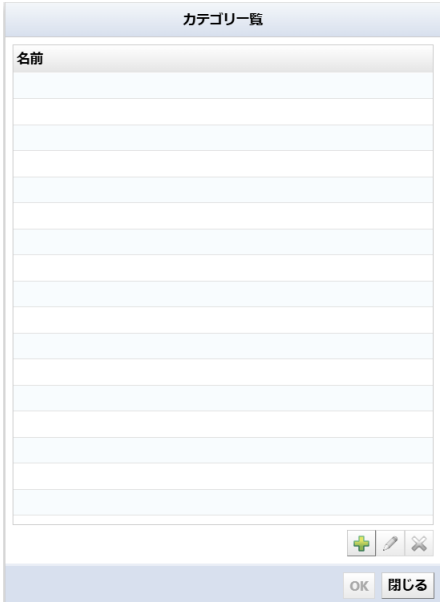
Playbook のカテゴリ機能は、Playbook を管理する際の利便性を向上させます。

- カスタムカテゴリの作成・編集
- Playbook 一覧でのカラータグによるラベル付け
- 1 つの Playbook 内での複数カテゴリ作成

(1) Playbook カテゴリの作成

1. ［Playbook］タブを開きます。
2. “Playbook”タイトルの横にある  ボタンをクリックすると「カテゴリー覧」ウィンドウが開きます。





3.  ボタンをクリックすると「カテゴリを追加」ウィンドウが開きます。

4. デフォルト画像ボタンをクリックしてカテゴリ用の SVG 形式のアイコン画像を選択します。
5. カテゴリ名を入力します。
6. [OK]ボタンをクリックし、続けて[閉じる]ボタンをクリックします。

(2) Playbook カテゴリの編集

1. “Playbook”タイトルの横にあるボタンをクリックし「カテゴリ一覧」ウィンドウを開きます。
2. 「カテゴリ一覧」ウィンドウでカテゴリ名をクリックします。
3. ボタンをクリックし「カテゴリを編集」ウィンドウを開きます。

4. 編集が完了したら、[OK]をクリックします。

(3) Playbook カテゴリの削除

1. “Playbook”タイトルの横にある ボタンをクリックし「カテゴリー覧」ウィンドウを開きます。
2. 「カテゴリー覧」ウィンドウでカテゴリ名をクリックします。
3. ボタンをクリックすると「カテゴリを削除」ウィンドウが開きます。

4. [はい]をクリックします。

6.12.4 Playbook の実行

Playbook を実行する方法について説明します。手動での実行から、スケジュール実行やトリガー実行など、さまざまな実行方法について説明します。

Playbook は[承認機能]の対象となるため、ユーザの権限や Playbook の承認状態により[Playbook を実行する]ボタンが無効化されている場合があります。

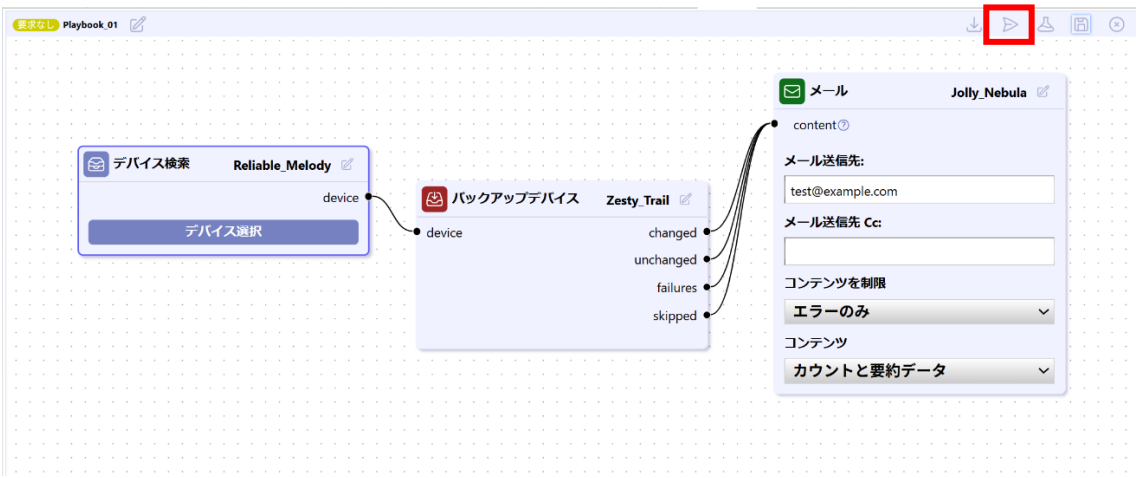
- 承認機能に関する権限は、以下の 2 つの権限内容です。

権限	説明
ツールの実行を承認する権限	承認要求（承認依頼）されたジョブを承認することができる権限。
承認なしにツールを実行する権限	承認要求（承認依頼）することなく、ジョブを実行することができる権限。

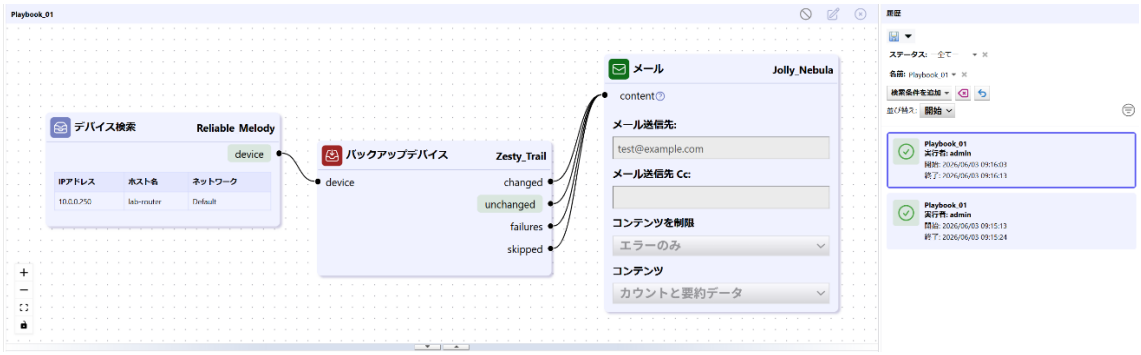
6.12.4.1 手動で実行

Playbook を手動で実行する手順は以下のとおりです。

1. ［Playbook］タブを開きます。
2. 実行する Playbook を選択してダブルクリックするか、［編集］ボタンをクリックします。
3. ［Playbook を実行する］ボタンをクリックします。

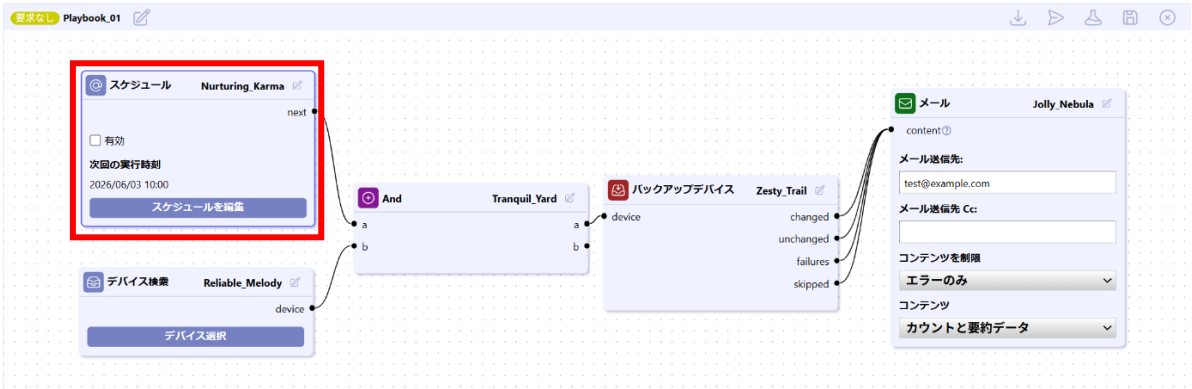


4. Playbook が実行されると、自動で実行画面に移動します。



6.12.4.2 スケジュール実行

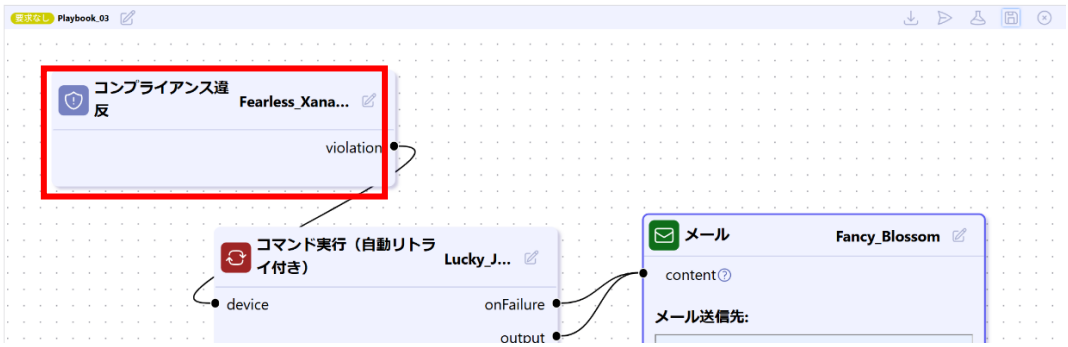
スケジュールに従って Playbook を自動的に実行します。スケジュール実行を設定するには、スケジュールノードを使用します。



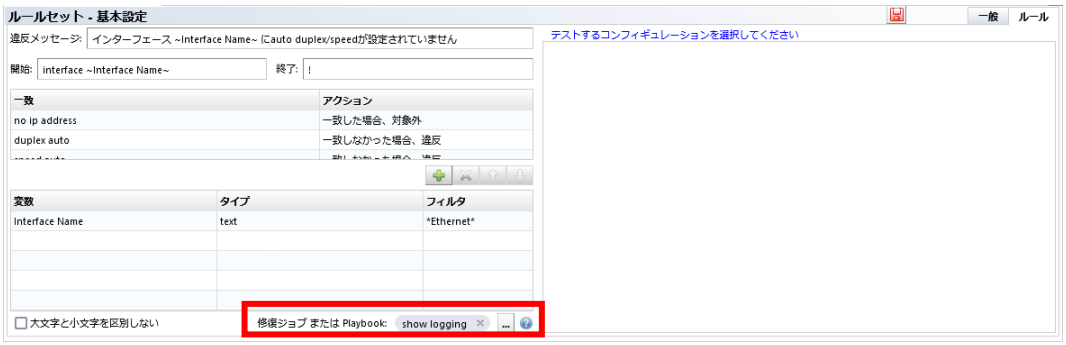
6.12.4.3 コンプライアンス違反検知時に実行

コンプライアンス違反を検知した際に Playbook を実行します。これを実行するには、コンプライアンスノードを使用し、作成した Playbook をコンプライアンスのルールセットに指定する必要があります。

1. Playbook にコンプライアンス違反ノードを追加します。



2. ［コンプライアンス］→［ルールセット］から任意のルールセットに「Playbook 実行」アクションを追加します。

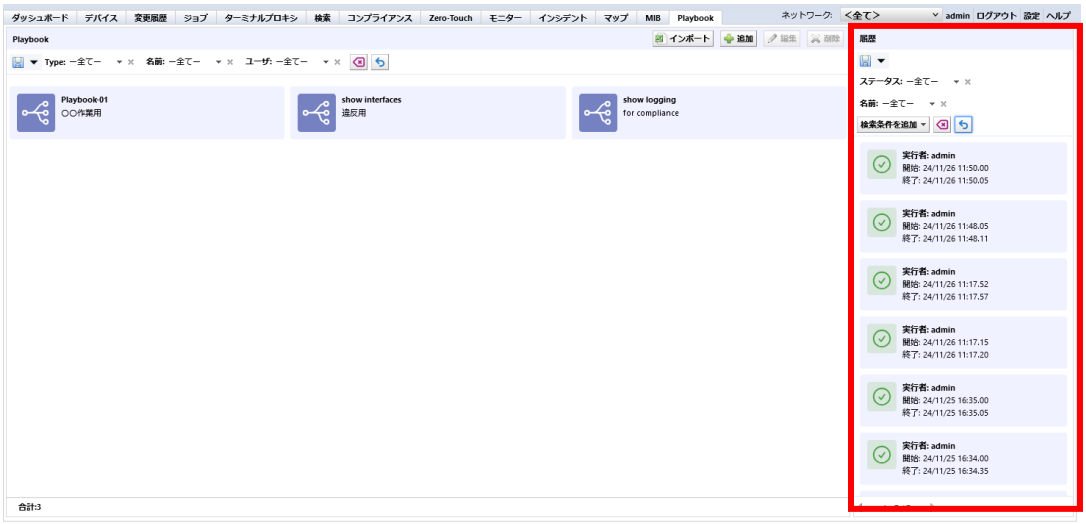


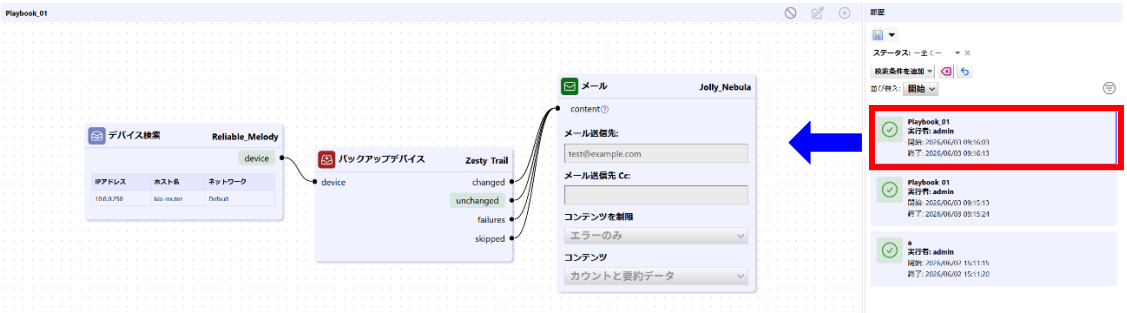
6.12.4.4 承認ログの表示

1. [Playbook]メインタブをクリックします。
2. 対象の Playbook をダブルクリックします。
3. ノードパネルの右側にある[ジョブ承認ログ]  をクリックします。

6.12.4.5 実行履歴

Playbook の実行履歴は、画面右側に表示されます。履歴から任意の Playbook をクリックすると、詳細情報を確認できます。



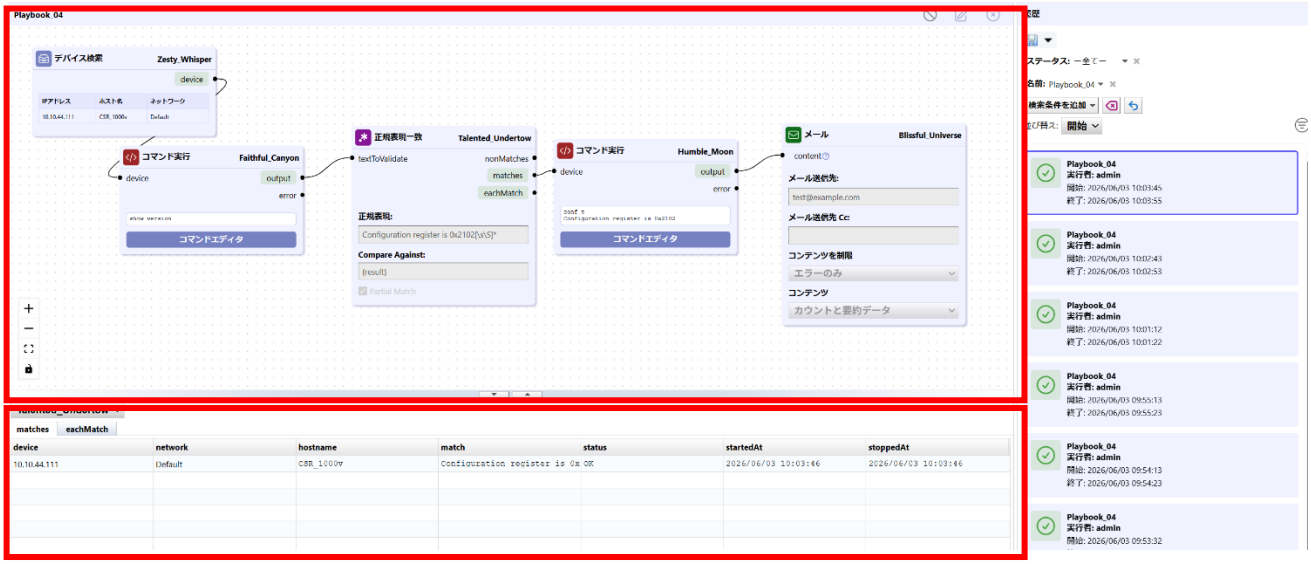


6 基本ツール

履歴確認画面は、大きく 2 つのセクションに分かれています。

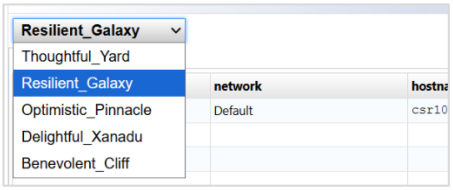
画面上部では、実行時の Playbook が表示され、実行中に出力があったノードは緑色で強調表示されます。

ノードをクリックすると画面下部のパネルがそのノードを出力結果に切り替わります。

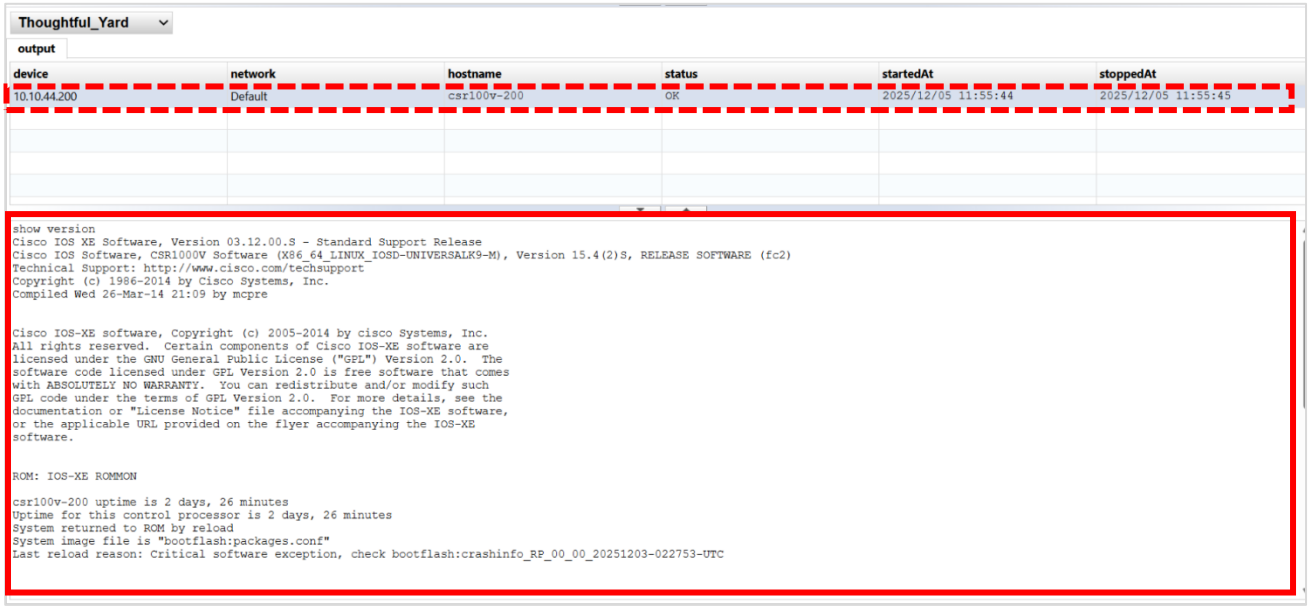


画面下部のパネルでは各ノードの出力が表形式で表示されます。選択したノードに 1 つ以上の出力がある場合は、タブが複数表示され、それぞれのタブに表形式で表示されます。

パネル上部で確認したいノードを選択表示することができます。ノードを選択すると画面上部の Playbook 画面で選択したノードが自動的にスクロールされます。



追加情報を持つ行を選択すると追加情報が表示するパネルが開きます。例えば、「コマンド実行」ノードの出力結果は行を選択するするとパネルが開き、結果が表示されます。



6.12.4.6 代替値の使用

多くのノードは主な結果とともにメタデータを出力します。「コマンド実行」ノードの場合、device や status などが含まれます。これらはすべて、Playbook の実行開始後にそのノードの出力テーブルで確認できます。フィールドが代替値に対応している場合、値を{中括弧}で囲むことでその値を参照できます。多くのノードでは、これらの値に対してテンプレート化された代替値をサポートしています。

ノード	設定可能フィールド
正規表現一致	正規表現と Compare Against で代替値を設定する事ができます。
コマンド実行	コマンドエディタで代替値を設定する事ができます。
コマンド実行(自動リトライつき)	コマンドエディタで代替値を設定する事ができます。
SSH 実行	コマンドで代替値を設定する事ができます。
変数の設定	値で代替値を設定する事ができます。
フィールド編集	カスタムフィールドで代替値を設定する事ができます。
ファイルアップロード	サーバからファイルを取得するコマンドで代替値を設定することができます。
コンプライアンス違反検出	メッセージで代替を設定する事ができます。

ある情報を独自のメタデータとして抽出し、ノードから列として出力したい場合、最も簡単な方法は「正規表現一致」ノードを使用することです。このノードは Java 形式の正規表現をサポートしており、名前付きマッチグループはその名前を持つ値として取り出されます。例えば Cisco デバイスの稼働時間を「uptime」という名前の値として抽出するには、`show version` コマンドの出力を、以下の正規表現を指定した正規表現一致ノードに渡します。

lab-router uptime is (?[¥w ,]+)

「Compare Against」がデフォルトの {result} に設定されている場合、この正規表現は「Compare Against」の値全体と一致するように設計されません。「Partial Match」を有効にして、正規表現の一部が少なくとも含まれていれば一致としてカウントするように指定しましょう。この設定を行うと、正規表現の一致結果には、一致した uptime が新しい「uptime」列に表示され、後続のノードで {uptime} として使用できます。

また、「Compare Against」を変更することで、これらを連鎖させてより具体的な情報を取得することも可能です。例えば、最近リセットされたスイッチを確認したい場合は、正規表現の一致条件に「day」を含めない稼働時間を確認することができます。「uptime」の正規表現マッチノードを新しい正規表現マッチノードに接続し、正規表現を day に設定します。「Compare Against」を{uptime}に設定し、「Partial Match」を有効にします。

その後、nonMatches の出力を確認するか、このノードを「Email」、「Webhook」、「コンプライアンス違反検出」、または「変数の設定」ノードに接続し、「デバイスが最近リセットされました：{uptime}」といったメッセージを設定することで、別の方法で結果を受け取ることができます。

6.13 バルクチェンジ

6.13.1 バルクチェンジの概要

「バルクチェンジ」とは「一括変更」という意味です。netLD のバルクチェンジ機能は、CLI コマンドのテンプレートの一部を変数に変換し、複数のネットワーク機器ごとに固有のパラメータに置き換えることで、複数のネットワーク機器に一括でコマンドを送信できる機能です。これにより、多数のネットワーク機器の設定を一括で変更できるため、設定変更にかかる時間を効率的に短縮できます。

たとえば、バルクチェンジを使用してネットワーク機器のパスワードやホスト名を変更する場合、個々の機器に手動でコマンドを送信する手間を省きつつ、セキュリティ要件に従って簡単かつ確実にネットワーク機器の設定を構成できます。また、アクセスリストやパスワードなどを定期的に変更する必要がある場合は、必要なコマンドをあらかじめテンプレートとして保存しておくと、繰り返し簡単に呼び出して実行できます。

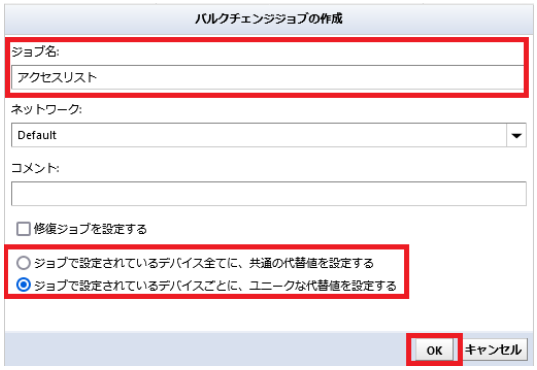
また、リビジョン 20240131.0729 から、バルクチェンジジョブで netLD を FTP/TFTP サーバまたは SCP クライアントとして使用することにより、OS の配布や証明書の配布を netLD 単体で実行できるようになりました。

6.13.2 バルクチェンジジョブを作成する

6.13.2.1 ケース 1

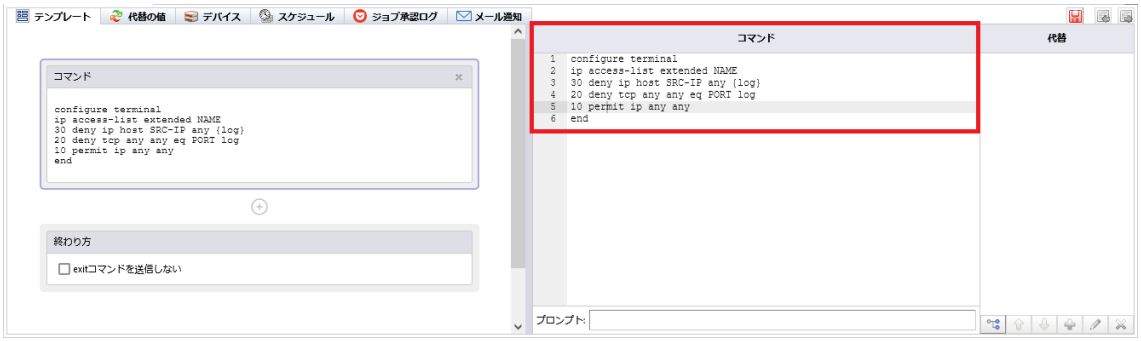
ここでは、「アクセスリストの設定->設定したアクセスリストの確認->インタフェースへの適用->running-config の確認」を例にバルクチェンジジョブを作成します。

1. [ジョブ]タブ→[ジョブ管理]サブタブを開きます。
2. [新しいジョブ]→[バルクチェンジ]の順にクリックします。
3. 任意のジョブ名を入力し、オプションを選択して、[OK]をクリックします。

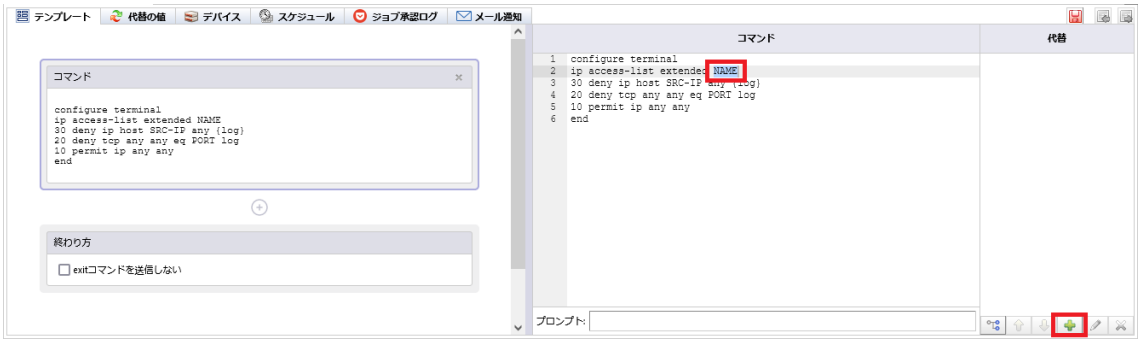


オプション	説明
修復ジョブを設定する	コンプライアンス機能で修復ジョブとして使用する場合にチェックを入れます。
ジョブで設定されているデバイス全てに、共通の代替値を設定する	ジョブの実行対象となるすべての機器に、同じ値を投入する場合に使用します。
ジョブで設定されているデバイスごとに、ユニークな代替値を設定する	ジョブの実行対象となる機器ごとに固有の値を投入する場合に使用します。

4. [テンプレート]タブの[コマンド]セクションに、デバイスに送信するコマンドを入力します。



5. 変数にしたい部分を範囲選択し、[代替]セクションの  ボタンをクリックします。

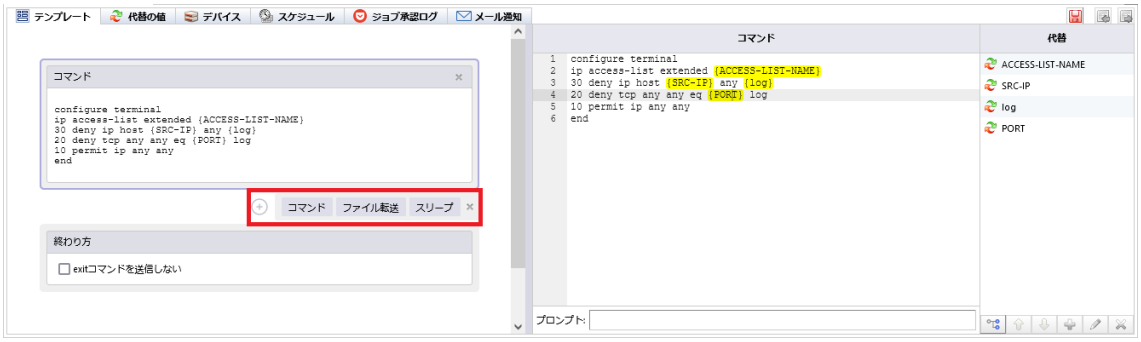


6. 名前欄に変数名を入力し、そのタイプとオプションを選択し[OK]をクリックします。

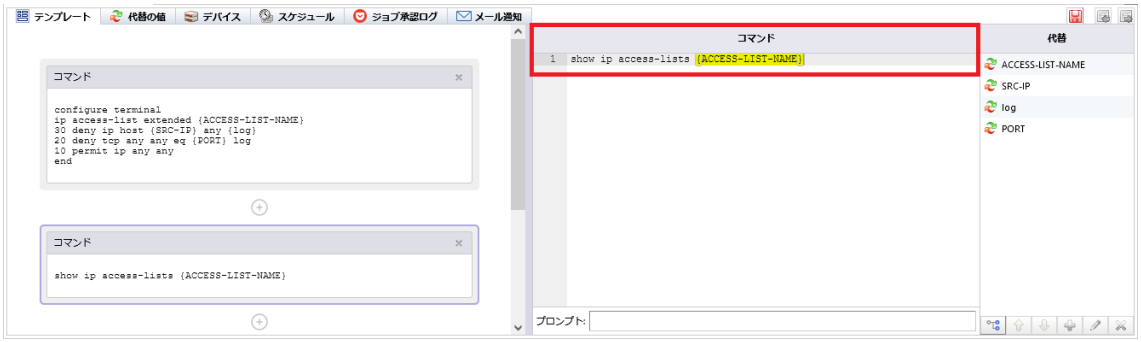
タイプ/オプション	説明
テキスト	代替値として任意のテキストを入力する場合に使用します。
IP アドレス	代替値として IP アドレスを入力する場合に使用します。 IPv4 または IPv6 形式ではない値を入力すると、値が無効であるというエラーが表示されます。
ホスト名	代替値としてホスト名を入力する場合に使用します。
IP アドレスまたはホスト名	代替値として IP アドレスまたはホスト名を入力する場合に使用します。
選択	ドロップダウンリストから代替値を選択したい場合に使用します。 設定する候補値があらかじめ決まっている場合に便利です。
条件選択	チェックボックス形式で、コマンドを含めるか含めないかを選択できるようになります。 チェックボックスをオフにすると、その代替値は空白の文字列として扱われます。
選択した値をデフォルトとして使用する	代替値を指定しない場合、テンプレート作成時のテキストを自動的に使用するようになります。

※ 変数として登録され、代替値に置き換え可能になった箇所は、黄色でハイライト表示されます。

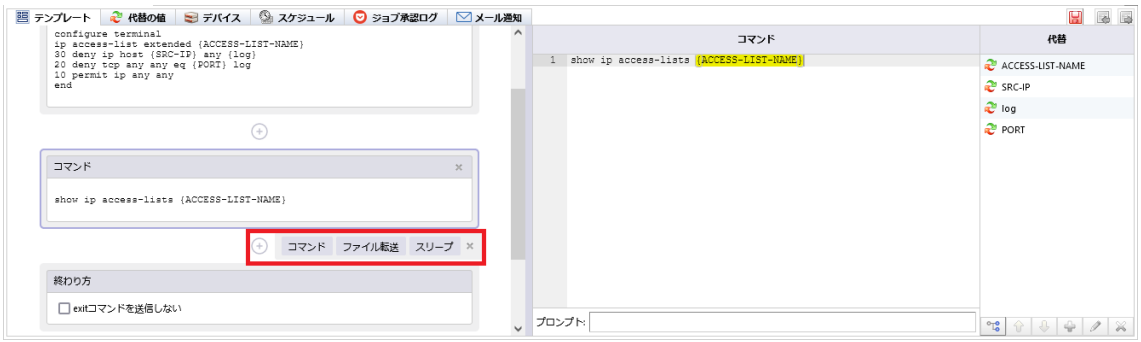
7. [+]をクリックし、「コマンド」を追加します。



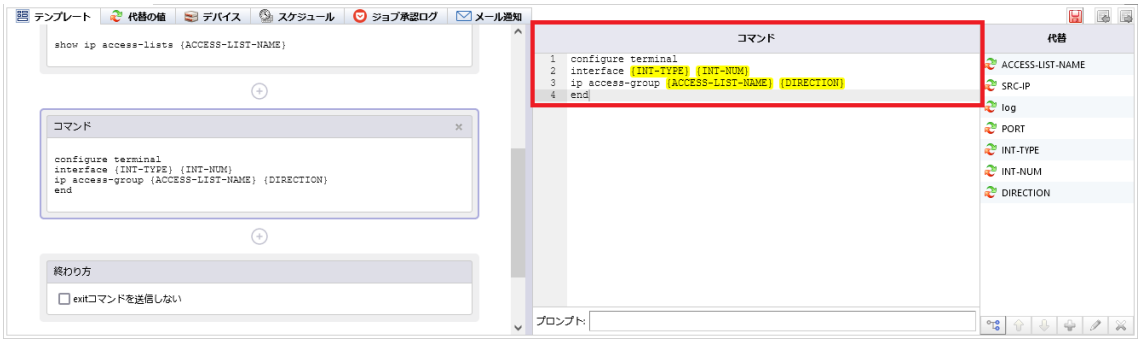
8. アクセスリストを確認するコマンドを入力します。



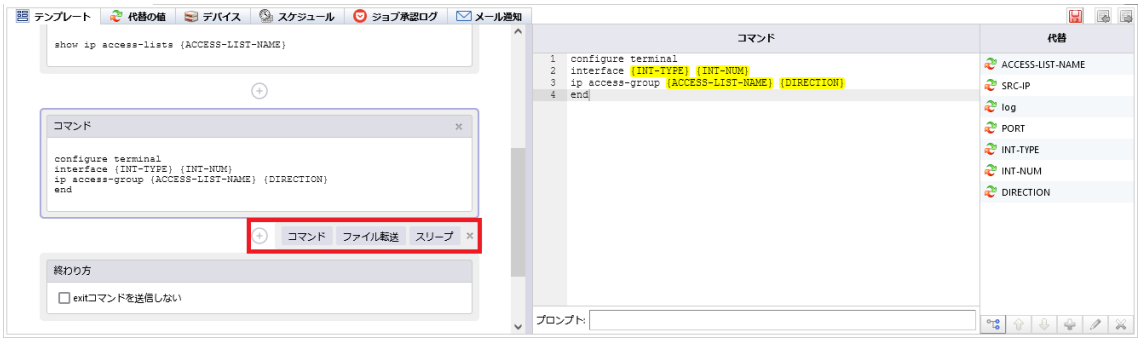
9. [+]をクリックし、「コマンド」を追加します。



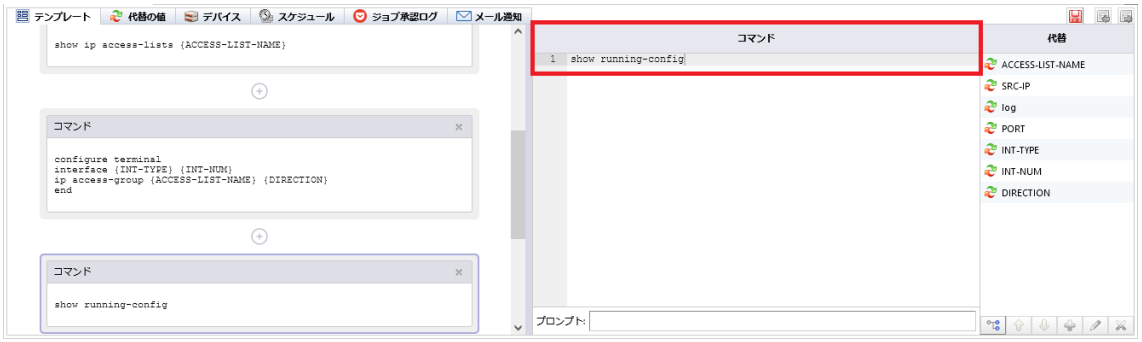
10. インタフェースにアクセスリストを適用するコマンドを入力します。



11. [+]をクリックし、「コマンド」を追加します。



12. running-config を確認するコマンドを入力します。



13. [デバイス]タブを開き、対象デバイスを指定します。

14. [代替の値]タブを開き、各変数を設定します。

※ 以下の画像は、[ジョブで設定されているデバイスごとに、ユニークな代替値を設定する]オプションで作成した場合の例で、デバイスごとに固有の値を入力できます。代替データは、Excel ファイルを使用してインポート()/エクスポート()することもできます。

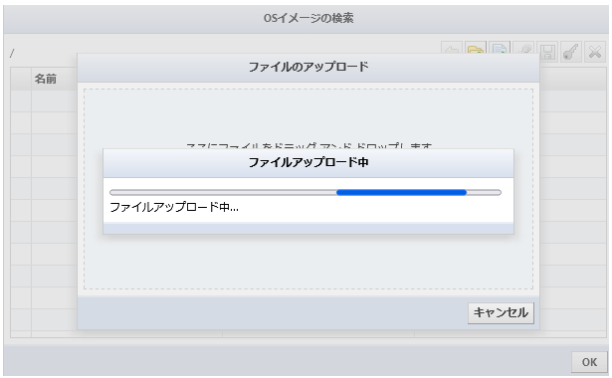
15.  ボタンをクリックし、ジョブを保存します。

6.13.2.2 ケース 2

ここでは例として、netLD を FTP サーバとして使用し、OS アップデートするためのバルクチェンジジョブを作成します。OS を配布する場合は、事前に機器ベンダーから OS イメージをダウンロードしてください。

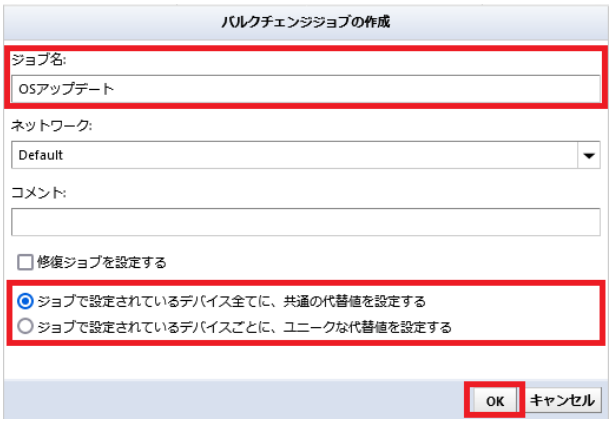
1. [インベントリ]タブ→[変更ツール]→[OS イメージ]をクリックします。
2. [+]をクリックします

3. 配布したい OS イメージを[ブラウス]から選択 または ドラッグ・アンド・ドロップし、netLD にアップロードします。

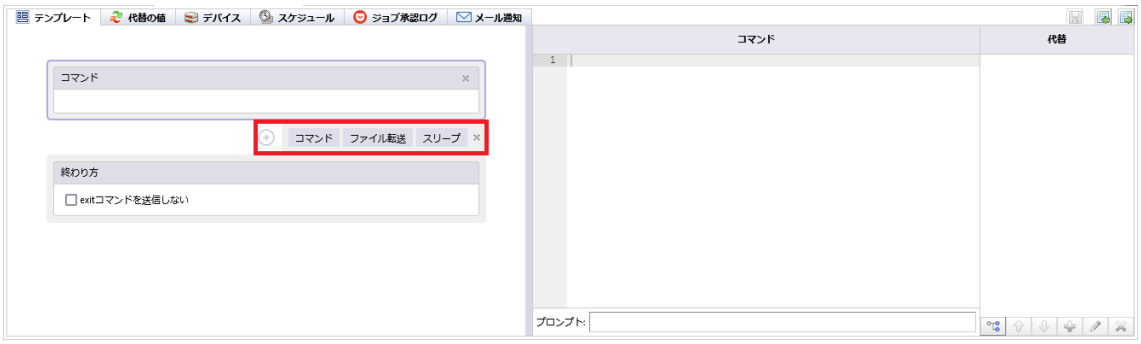


4. [OK]をクリックします。

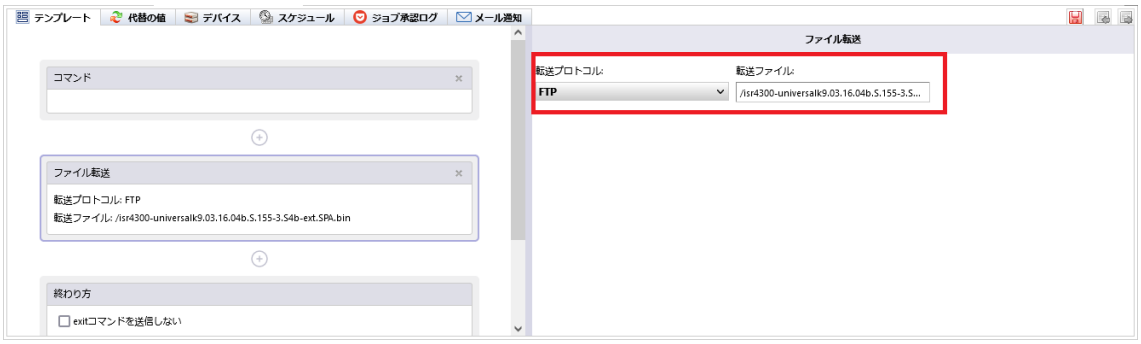
5. [ジョブ]タブ→[ジョブ管理]サブタブを開きます。
6. [新しいジョブ]→[バルクチェンジ]の順にクリックします。
7. 任意のジョブ名を入力し、オプションを選択して、[OK]をクリックします。



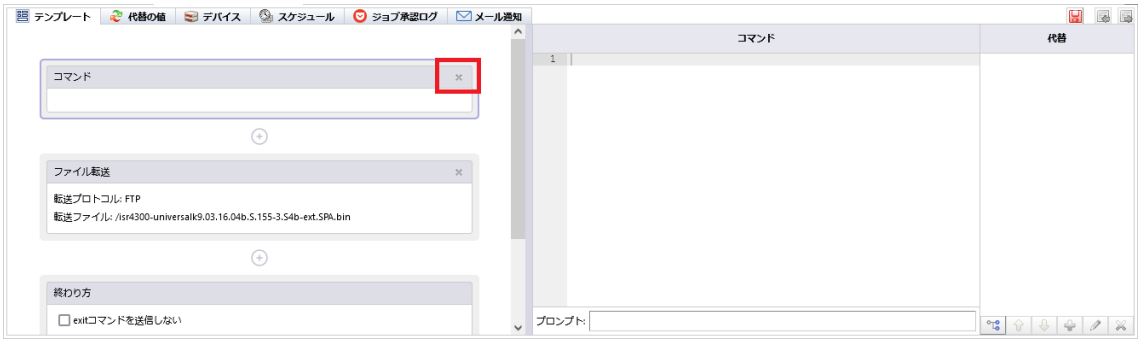
8. ［+］をクリックし、「ファイル転送」を追加します。



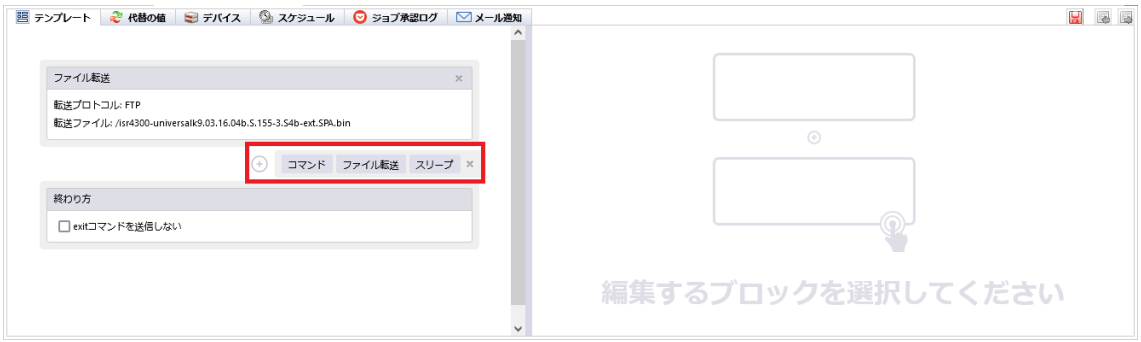
9. 「転送プロトコル」を選択し、手順 4 で追加した OS イメージを転送ファイルとして指定します。



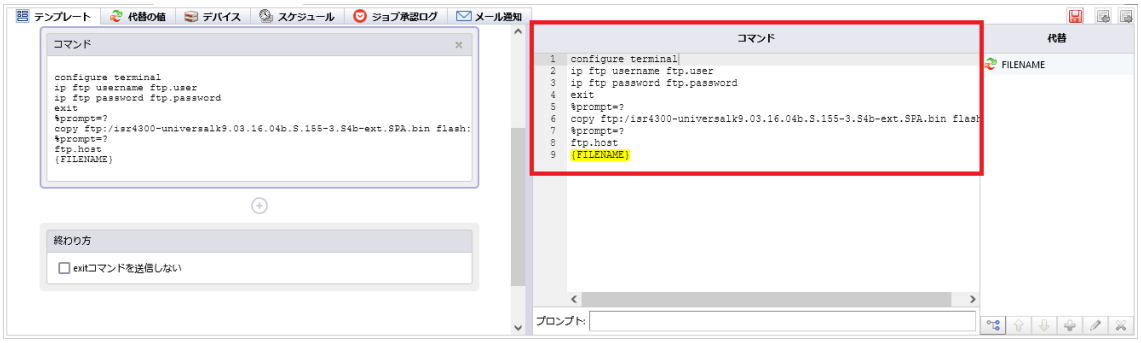
10. 一番上のコマンドを削除します。



11. ［+］をクリックし、「コマンド」を追加します。

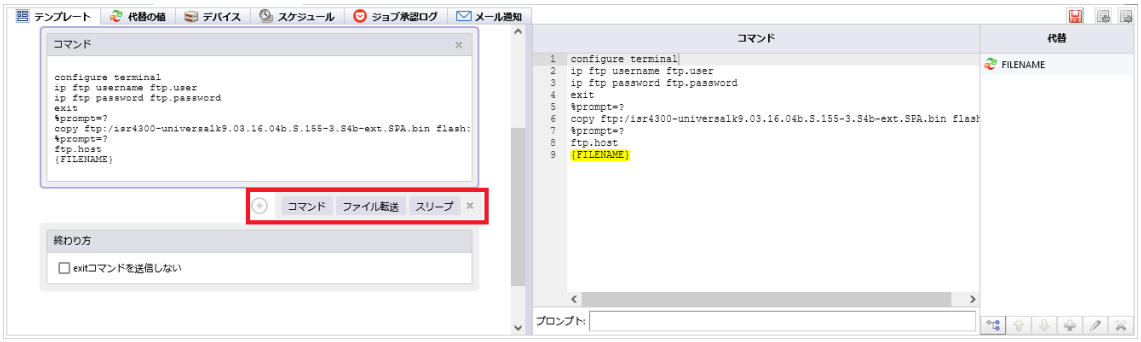


12. コマンド欄に、OS を取得するコマンド と OS を適用するコマンド を入力します。

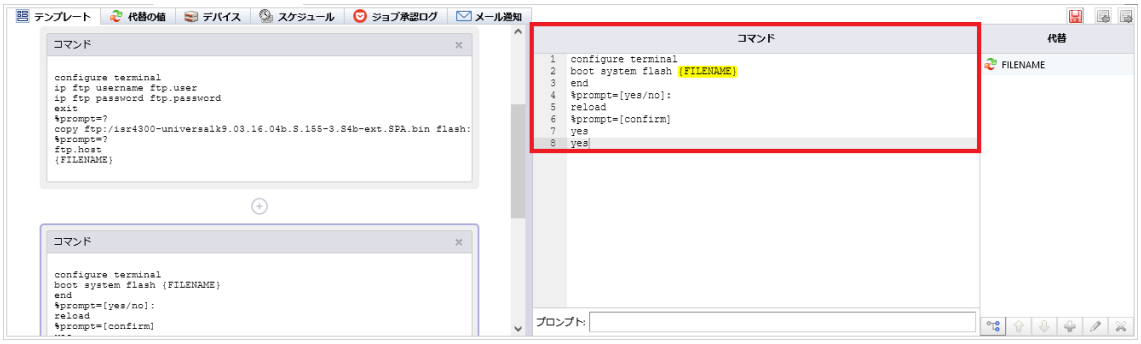


変数	説明
ftp.host / tftp.host	FTP/TFTP サーバとなる netLD のホスト名
ftp.username	FTP ユーザ名
ftp.password	FTP ユーザのパスワード

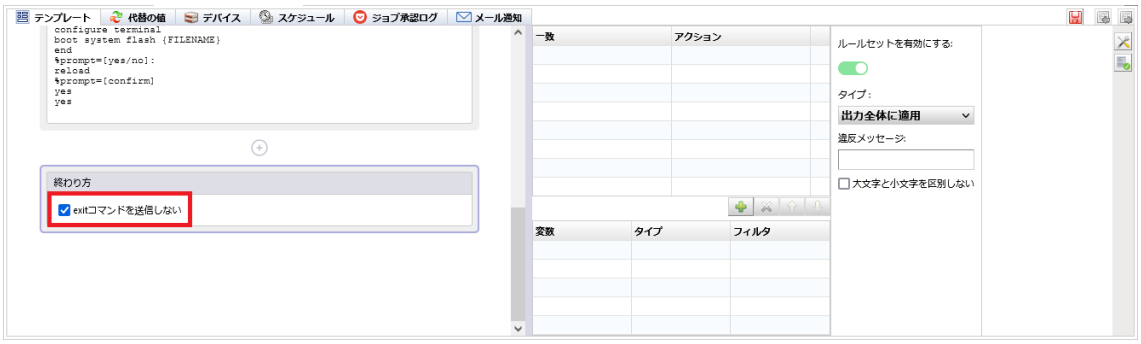
13. [+]をクリックし、「コマンド」を追加します。



14. コマンド欄にリロードするコマンドを入力します。



15. 「終わり方」をクリックし、「exit コマンドを送信しない」にチェックを入れます。



16. [デバイス]タブを開き、対象デバイスを指定します。

17. [代替の値]タブを開き、各変数を設定します。

※ 以下の画像は、[ジョブで設定されているデバイス全てに、共通の代替値を設定する]オプションで作成した場合の例で、すべてのデバイスに同じ値を使用します。代替データは、Excel ファイルを使用してインポート()/エクスポート()することもできます。

18.  ボタンをクリックし、ジョブを保存します。

6.13.3　バルクチェンジジョブを実行する

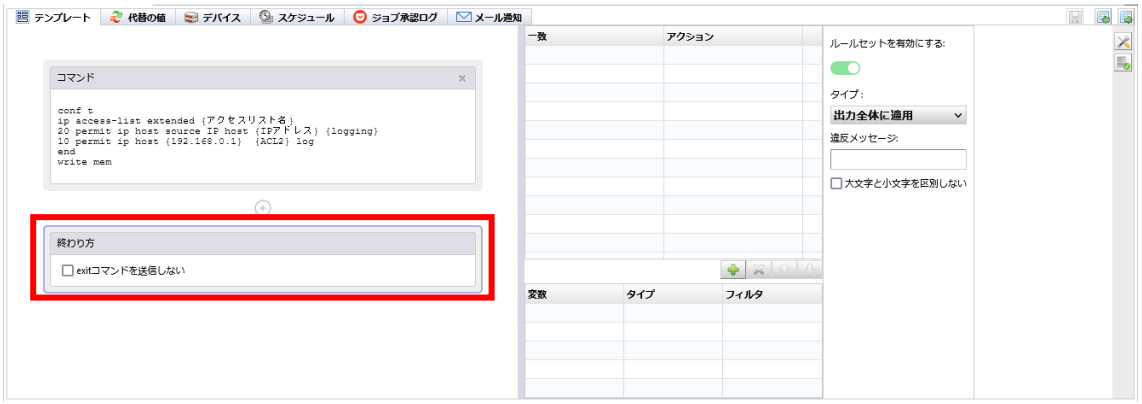
バルクチェンジジョブを実行するには、[ジョブ]タブ→[ジョブ管理]サブタブで実行したいジョブを選択し、[すぐに実行]ボタンをクリックします。

または、[デバイス]タブから実行することもできます。ツールメニュー→[バルクチェンジ]から作成したバルクチェンジジョブを選択し、クリックします。

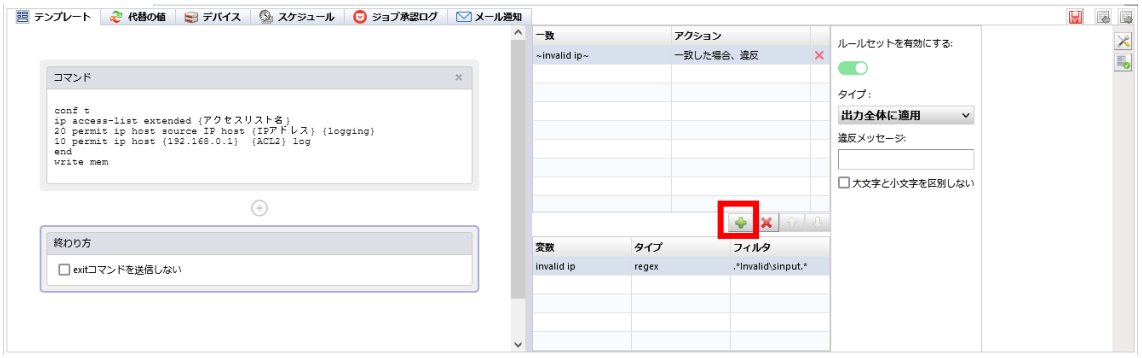
6.13.4　バルクチェンジジョブのルールセットを有効にする

ルールセット機能は、ユーザが指定したルールとバルクチェンジジョブの実行結果を比較して判定する機能です。実行結果に特定の文字列が含まれるかどうかなどのルールに基づいて判定します。判定結果は[ジョブ履歴]から参照します。

1. バルクチェンジの[テンプレート]タブで、画面左側のコマンドフローから[終わり方]をクリックします。



2.  ボタンをクリックし、ルール（一致/アクション）を設定します。

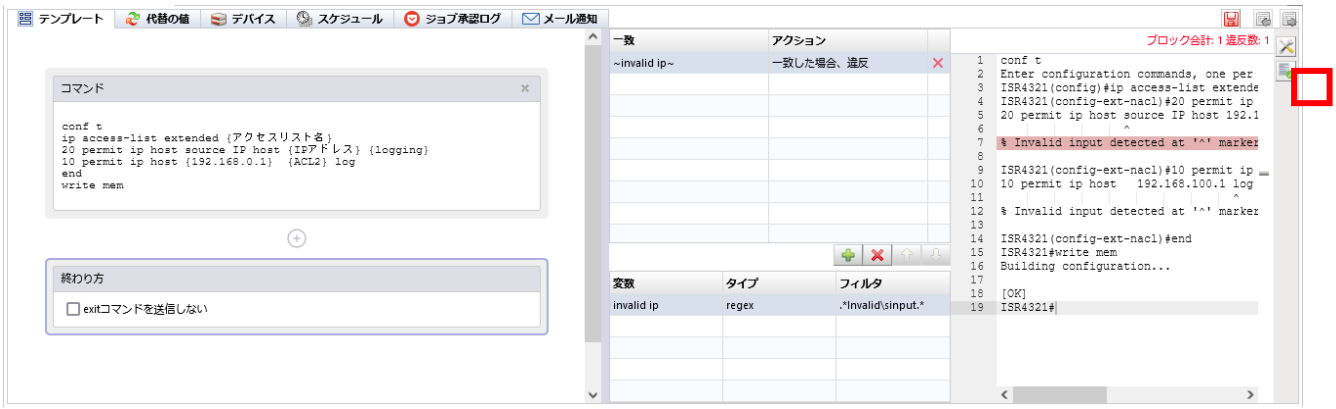


※　ルールの詳細については、6.1.3 コンプライアンスの概要を参照してください。

3. ルールセットを有効にします。

オプション		説明
タイプ	出力全体に適用	ジョブ実行結果全体に対し、ルールセットを有効にします。
	ブロックに適用	ジョブ実行結果から［開始]/[終了］に指定した文字の範囲（=ブロック）に対しルールセットを有効にします。
違反メッセージ		ルールに合致しなかった場合に表示するメッセージを入力します。
大文字と小文字を区別しない		有効にすると、ルールを判定する時に大文字/小文字を区別しなくなります。

追加したルールを任意の文字列に対してテストすることもできます。[評価を表示]ボタンをクリックし、[評価]セクションにテスト対象の文字列を入力してください。



4.  ボタンをクリックし、ジョブを保存します。

6.14 承認機能の概要

承認機能とは、申請者が作成・編集したジョブを、上長などの承認者が承認することで実行できるようになる機能です。承認を得ていないジョブは、実行できなくなります。この機能を利用することで、誤操作の防止やコンプライアンス強化など、セキュアな運用を実現できます。

※この承認機能は、ネットワーク機器の設定を変更するためのジョブに対してのみ有効です。

【承認の流れ】

1. 申請者がジョブを作成・編集し、[承認要求]を行う（承認依頼）
2. 承認担当者が、該当ジョブ内の[ジョブ承認ログ]から承認依頼を確認する。
3. 問題がなければ[承認]を行う。問題があれば確認画面から[却下]または[コメント]を行い、申請者へ連絡する。
4. [承認]が行われたら、申請者は該当ジョブを実行する。

6.14.1 承認機能の権限を設定する

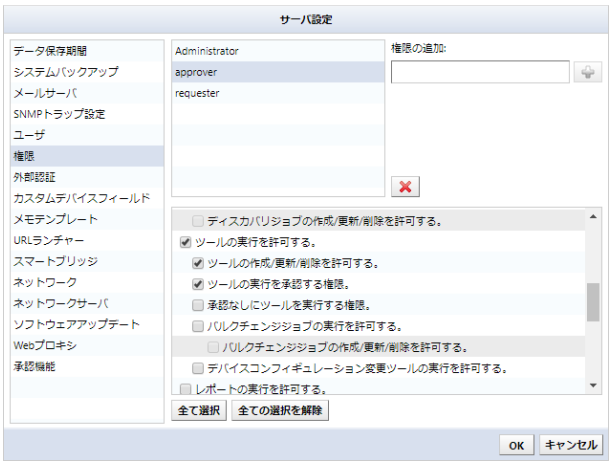
登録済みの権限に対して、承認者の設定をします。設定された権限を割り当てられたユーザが、ジョブの承認を行うことができます。

1. [設定]をクリックします。
2. [権限]を選択し、対象の権限を選択します。
3. 権限内容を指定し、[OK]をクリックします。

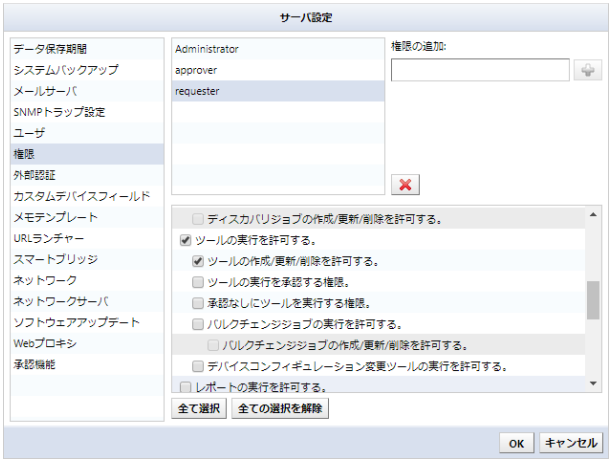
承認機能に関する権限は、以下の 2 つの権限内容です。

権限	説明
ツールの実行を承認する権限。	承認要求（承認依頼）されたジョブを承認することができる権限。
承認なしにツールを実行する権限。	承認要求（承認依頼）することなく、ジョブを実行することができる権限。

■承認者の権限を設定する場合、「ツールの実行を承認する権限。」にチェックを入れます。



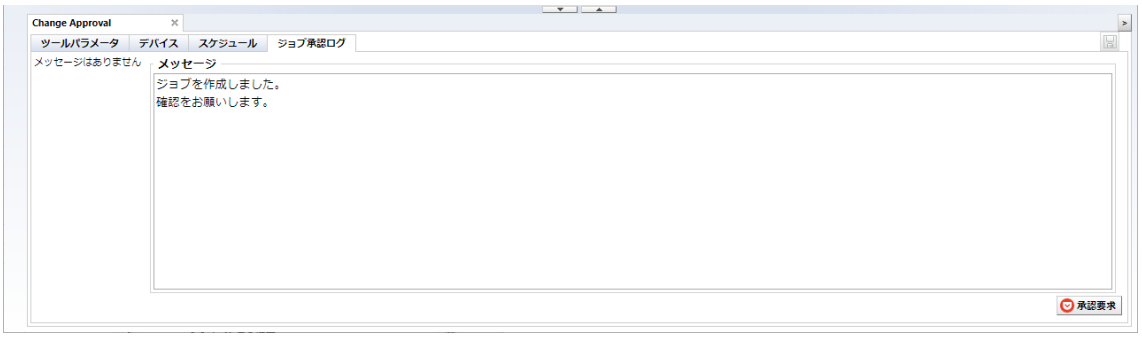
■申請者の権限を設定する場合、「ツールの実行を承認する権限。」のチェックをはずします。



6.14.2　承認要求を申請する（ジョブを申請する）

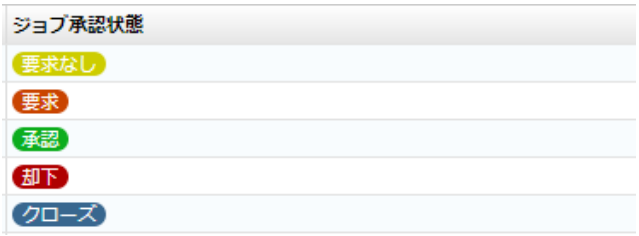
申請者はジョブを作成・編集する際に、承認要求を申請することができます。

1. ジョブを作成・編集します。
2. [ジョブ承認ログ]タブを開き、メッセージ欄にメッセージを入力し、[承認要求]をクリックします。



申請が完了すると、[ジョブ承認状態]カラムに「要求」と表示されます。

■[ジョブ承認状態]カラムの表示例



■[ジョブ承認状態]カラムの表示内容一覧

ジョブ承認状態	説明
要求なし	ジョブ承認要求が設定されていません。
要求	ジョブ実行承認が要求されています。
承認	ジョブ実行が承認されています。
却下	ジョブ承認要求が却下されています。
クローズ	ジョブがクローズされています。このステータスは以下の場合に設定されます。 ジョブの実行 管理者/ジョブ要求者によるクローズ ※クローズされたジョブを実行したい場合は、再度承認要求を行う必要があります。

6.14.3　承認要求を承認する（ジョブを承認する）

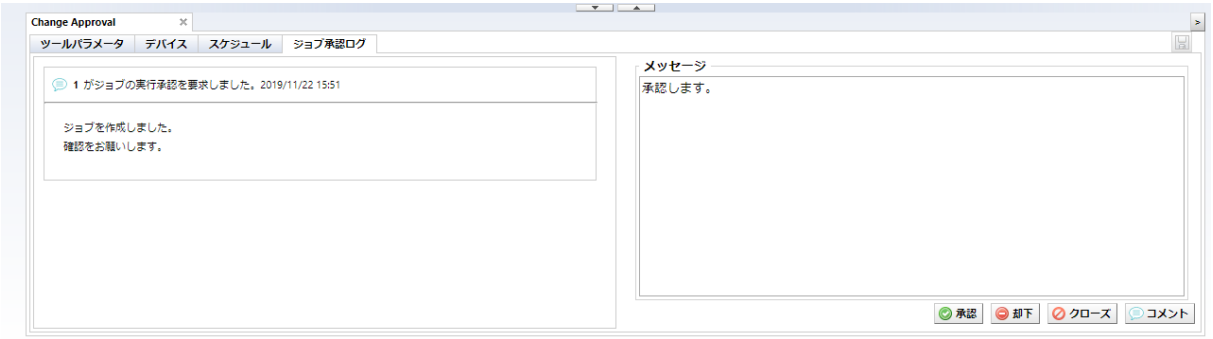
承認者は、申請者から申請されたジョブ（承認要求）を承認することができます。

1. [ジョブ管理]タブを開きます。
2. 承認要求されたジョブを開きます。

   [ジョブ管理]画面上部にある「ジョブ実行承認状態」から、表示するジョブをフィルタできます。

3. ジョブ内容を確認し、[ジョブ承認ログ]タブを開きます。
4. メッセージ欄にメッセージを入力し、[承認]をクリックします。

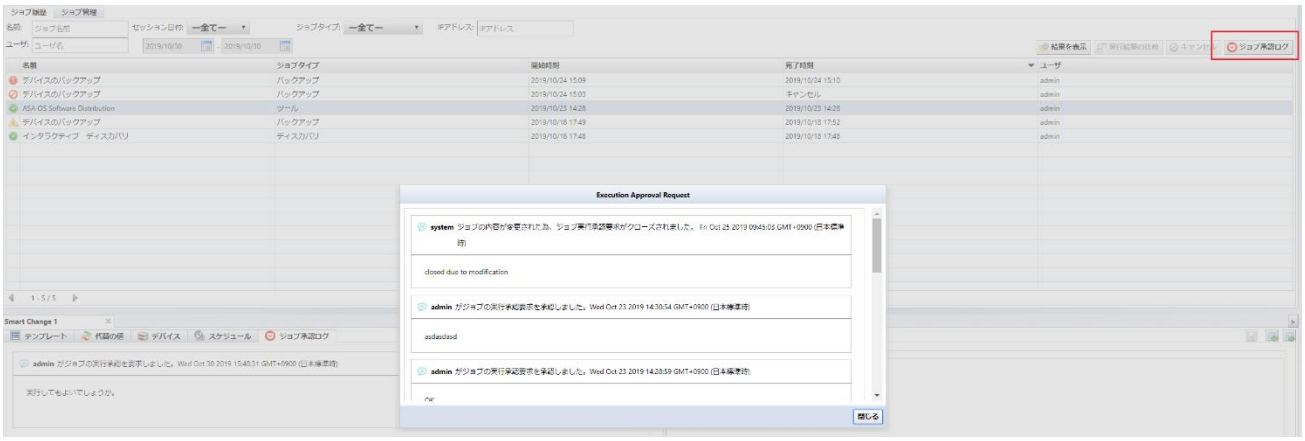
   問題があれば、メッセージ欄にメッセージを入力し、[却下]または[コメント]をクリックします。



6.14.4　承認までの記録を確認する

[ジョブ履歴]画面で、対象ジョブを選んで[ジョブ承認ログ]をクリックすると、承認までの記録（メッセージ）を確認することができます。

※[ジョブ承認ログ]ボタンは、承認後に実行されたジョブの場合にのみ有効になります。



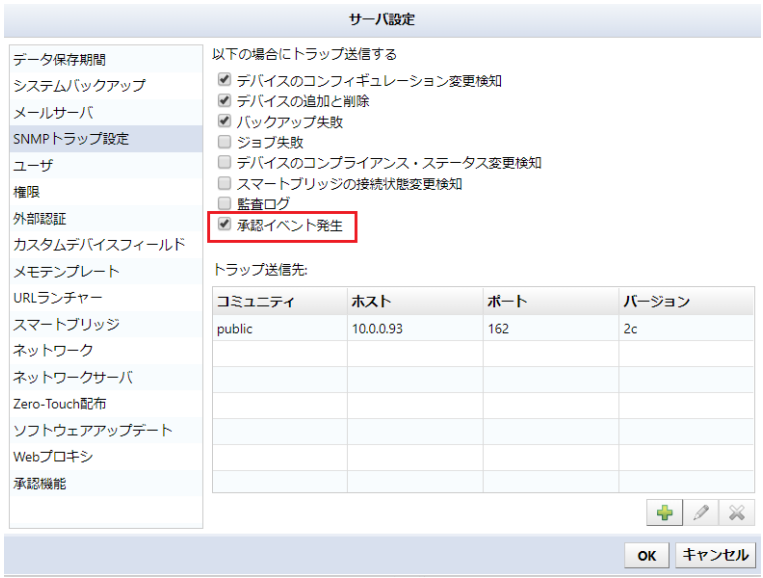
6.14.5　承認機能の通知

ジョブの申請、実行、完了時に SNMP トラップまたは該当のジョブ関係者へメールによる通知を行うことができます。

6.14.5.1 SNMP トラップ設定

サーバ設定画面の SNMP トラップ設定から、承認イベント発生時にトラップを送信します。

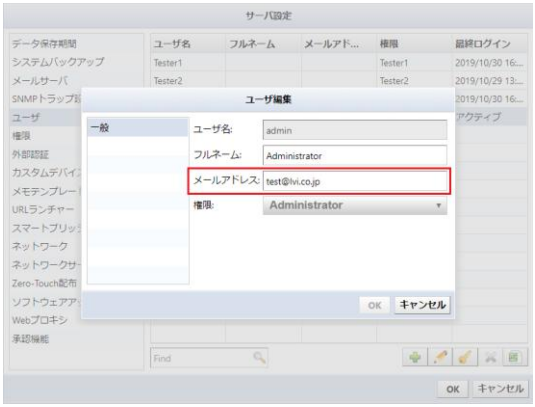
ジョブの要求/実行/承認/却下/クローズ時にトラップが送信されます。



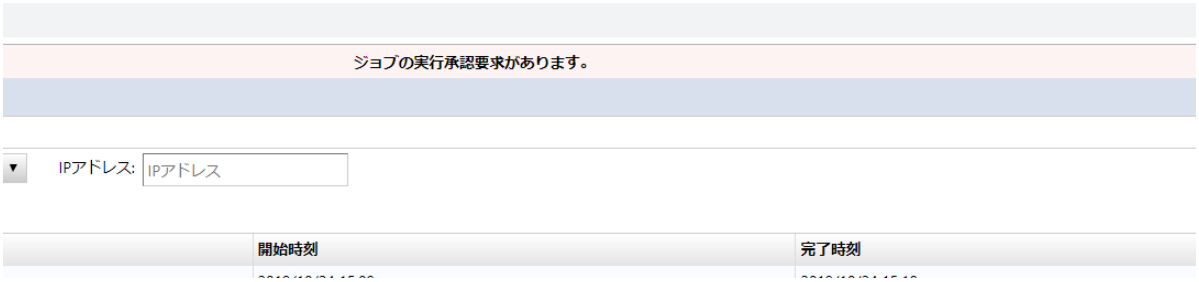
6.14.5.2 メール送信

サーバ設定画面のユーザ編集でメールアドレスを設定することで、承認イベント発生時にメールを送信することができます。ジョブの要求/実行/承認/却下/クローズ時にメールが送信されます。

メール送信を行うためには、事前にメールサーバを設定しておく必要があります。

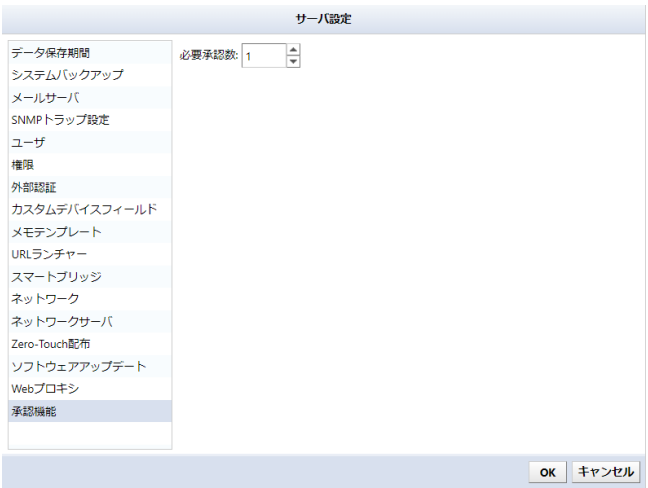


また、ジョブの承認要求がある場合、画面上部に以下のようなバナーが表示されます。



6.14.6 必要承認数を変更する

申請者が作成・編集したジョブを実行できるようになるまでに必要な承認数を指定できます。必要承認数の設定は、[設定]→[承認機能]より設定できます。設定可能な範囲は、1～3 です。



6.15 コンプライアンスの概要

コンプライアンスポリシーを設定すれば、管理者は自動的にいずれかのデバイスのコンフィギュレーションが間違っていることを通知されます。この機能は、ネットワークの安定性・堅牢性を保つ大きな助けとなります。違反が起こったときは、ステータス表示、円グラフ、トラップハンドラが役に立ちます。状況を判断して問題を解決するのに少ない時間で済みます。間違った、安全でないコンフィグを自動的に検出するためには、コンプライアンスルールというものを作らなくてはいけません。一つのルールは、以下のマッチング条件を用いて構成されます。それぞれの条件は一つの検索文字列を持っており、netLD は与えられたコンフィギュレーションがその文字列にマッチするかを調べます。

ジョブ承認状態	説明
一致した場合、対象外	文字列がコンフィグに当てはまる場合，まだチェックしていない残りのルールにかかわらず、このコンフィグは安全だと言えます。
一致しない場合、対象外	文字列がどのコンフィグの行にもマッチしなかった場合、まだチェックしていない残りのルールにかかわらず、このコンフィグは安全だと言えます。
一致した場合、違反	コンフィギュレーションが条件に当てはまった場合、そのコンフィグをルール違反とします。
一致しなかった場合、違反	文字列がどのコンフィグの行にもマッチしなかった場合、違反にします。

言い換えれば、"...違反" はブラックリスト、"...対象外" はホワイトリストです。 これらの基礎ルールを組み合わせ、様々なルールを追加することができます。

コンプライアンスルールを集めたものは *ルールセット*と呼びます。ルールセットもまた、自由に作成することができます。ただし、netLD には「よくある」典型的なルールセットがすでに用意されております。すべてのデフォルトであるルールセットは、11 デフォルトで存在するコンプライアンスルールを参照してください。

さらに、もっと大きな単位でコンプライアンスを管理するために、*ポリシー*というものが備わっています。デバイスに適用するものは実際にはこれです。ポリシーはルールセットを複数組み合わせて作られますが、加えて*それを適用するデバイスのリスト*や、*違反の重大さ*(エラーまたは警告または通知)、違反の履歴などの情報も持っています。

ルール、ルールセットおよび ポリシーを作ることができる場所は、*コンプライアンスタブ*のサブタブです。サブタブをいくつか概観してみましょう。

6.15.1 ルール

ルールセットサブタブ

ルールセットサブタブ(メインペイン)はルールセットを管理します。

ルールセット	アダプタ	コンフィギュレーション
IOS Session Idle Timeout	Cisco IOS	/running-config
IOS Secure Enable Passwords	Cisco IOS	/running-config
IOS SSH-only Restricted Access	Cisco IOS	/running-config
IOS Interface Auto-Duplex/Speed	Cisco IOS	/running-config
IOS Disabled Unneeded Services	Cisco IOS	/running-config
IOS Telnet Restricted Access	Cisco IOS	/running-config

ルールサブタブ

*ルールセット*サブタブでそれぞれのルールセットをダブルクリックすると、その内容がステータスペインの新たなタブに表示されます。新しいタブには 2 つのサブタブ、*一般*サブタブと*ルール*サブタブがあります。

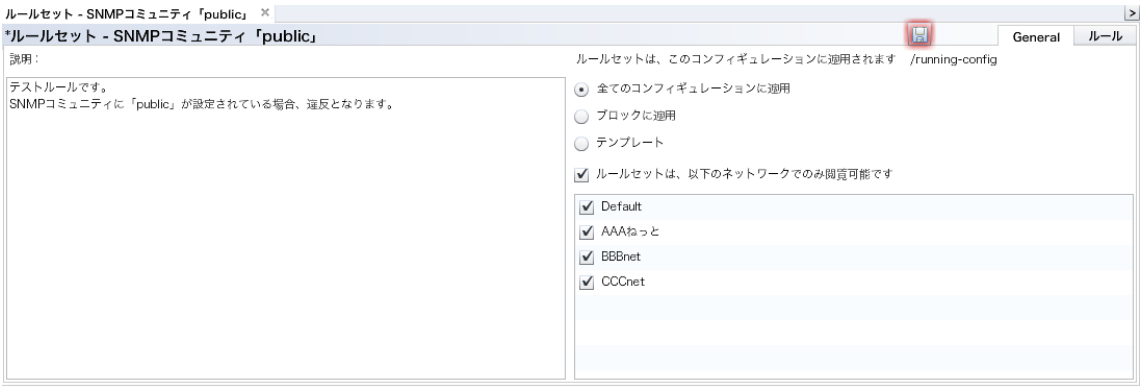
項目	説明
違反メッセージ	ルールに違反した場合に表示されるメッセージを入力します。
開始/終了	この欄は、ルールセットの設定によっては現れません。表示されるのは、一般サブタブでブロックに適用ルールが選択された時のみです。この場合、検索は最初にこの開始・終了テキストから行われ、コンプライアンス違反はその範囲のテキストに対してのみチェックされます。
一致	検索される文字列です。
アクション	どの基礎ルールを適用するかを選びます。 一致しない場合、対象外 一致した場合、対象外 一致しなかった場合、違反 一致した場合、違反
変数	マッチクエリ内で使える変数を入力します。変数名が X のとき、その値は~X~で用いることが出来ます 検索条件に変数が現れた場合、マッチする文字列が変数に入ります。同じ変数が一つの検索条件に複数回、あるいは複数の検索条件に複数回現れた場合、はじめの値が用いられます。
タイプ	マッチする可能性のある 4 つのタイプを指定します。タイプにマッチしない場合、検索条件から外れます。 テキスト ： すべてのテキストがマッチします。

項目	説明
	IP アドレス ： IP アドレスを表す文字列のみにマッチします。 ホスト名 ： ホスト名にマッチします。 ワード ： 単語にマッチします。 正規表現 ： 正規表現を使用してマッチする文字列をさがします。
フィルタ	検索する文字列や値を入力します。*が入力された場合、「どのような値でも良い」という意味になります

一般サブタブ

一般サブタブは、ルールの説明や適用範囲を設定するタブです。ルールに対する説明を書くことは、後のメンテナンスの上で重要です。現在の管理者が退職した場合を考えてみてください。コンプライアンスを適切に管理するためには、後任の者が書かれたルールを理解しなくてはなりませんが、一般的には、ルールの定義だけからそのルールの目的を推測することは極めて難しいことです。どのようなことが起こっても安定したメンテナンスを行うために、ルールには最悪でも最低限の説明を加え、出来ればわかりやすい説明を加えます。

現在選択しているルールの説明を加えることができる他、ルール自体の設定を行うことも出来ます。



項目	説明
説明	ルールの説明を入力します。
全てのコンフィギュレーションに適用	コンフィギュレーション全体にルールを適用します。
ブロックに適用	コンフィギュレーションをブロック単位に分け、ブロッグ単位でルールを適用します。
テンプレート	コンフィギュレーションをテンプレート上から 1 行ずつ比較し、差分がある場合は違反になります。
ルールセットは、以下のネットワークでのみ閲覧可能です	チェックを有効にした場合、ルールの適用対象となるネットワークが制限されます。

新規ルールの作成

ここでは、スクリーンショットを交えて新規ルールの作成方法をお伝えします。例として Cisco IOS のデバイスコンフィギュレーションで SNMP コミュニティ設定が"public"である場合に違反を発生させてみましょう。

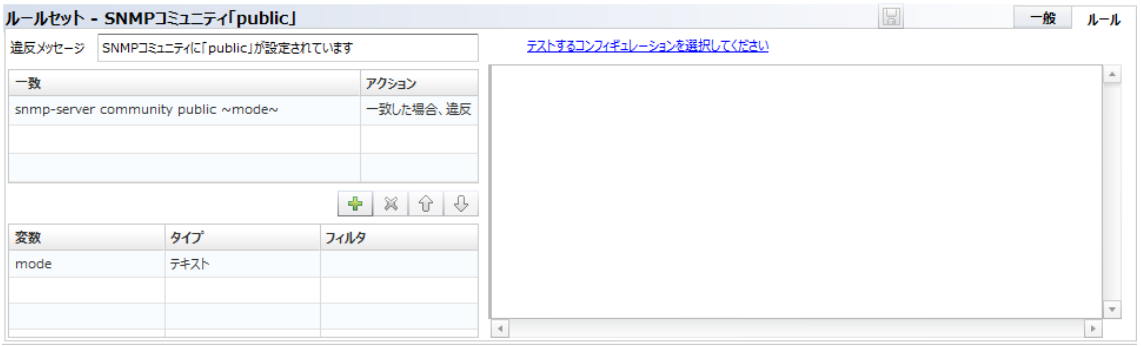
コンプライアンス→ルールセットタブで 作成 ボタンを押してください。

ルールの名前、対象アダプタ(機種の分類)、どちらのコンフィギュレーションに適用するルールであるか(running-config か startup-config か)を選び、OK ボタンを押してください。

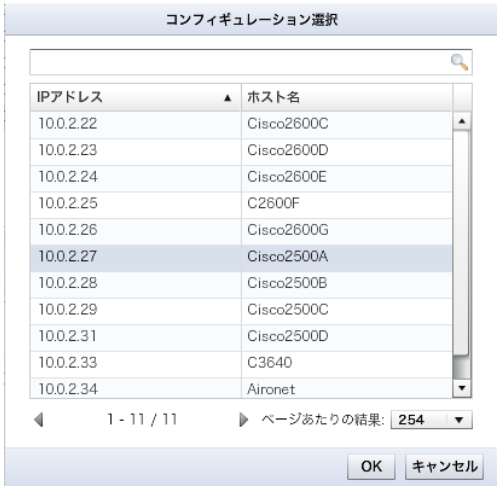
違反メッセージ欄に、違反検出時に表示されるメッセージを入力してください。この例では、メッセージは「SNMPコミュニティに「public」が設定されています」です。終わったら、ボタンを押してください。

一致に、違反となるテキストを入力し、アクションで「一致した場合、違反」を選択します。

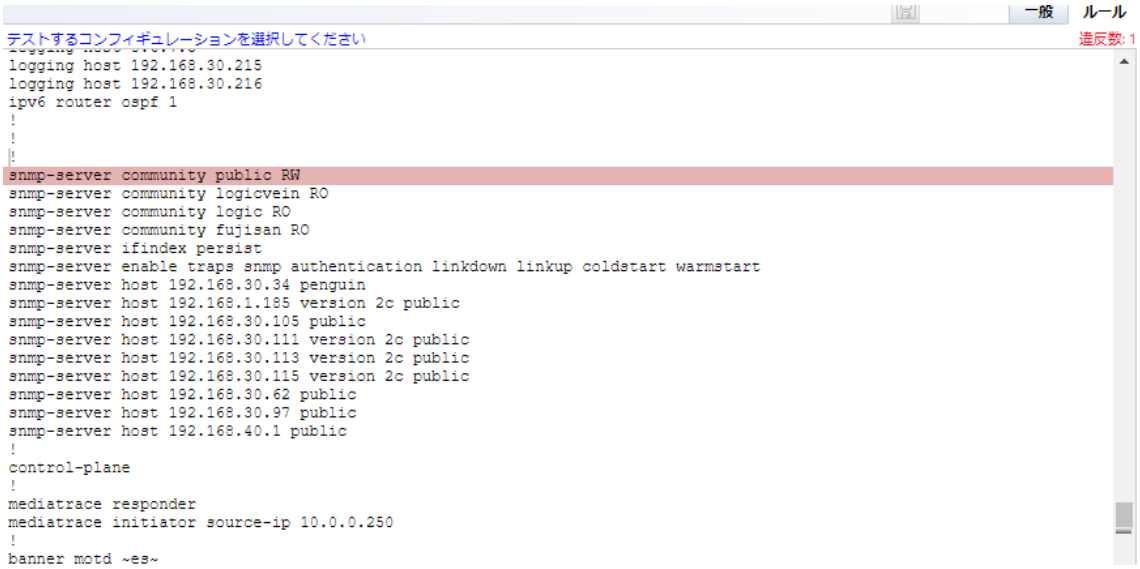
作成したルールをテストする場合、テストするコンフィギュレーションを選択してくださいをクリックして、インベントリからコンフィギュレーションを選択してください。



ルール作成時に選択したアダプタに当てはまるデバイスのリストがコンフィギュレーション選択ウィンドウに一覧表示されます。この列では、始めに選択した IOS アダプタに合致するデバイスのみが表示されます。



このテキストルールに対して違反が検索され、そしてもし違反が見つかれば赤で表示されます。終わったら、次の章でこのルールセットからポリシーを作りましょう。



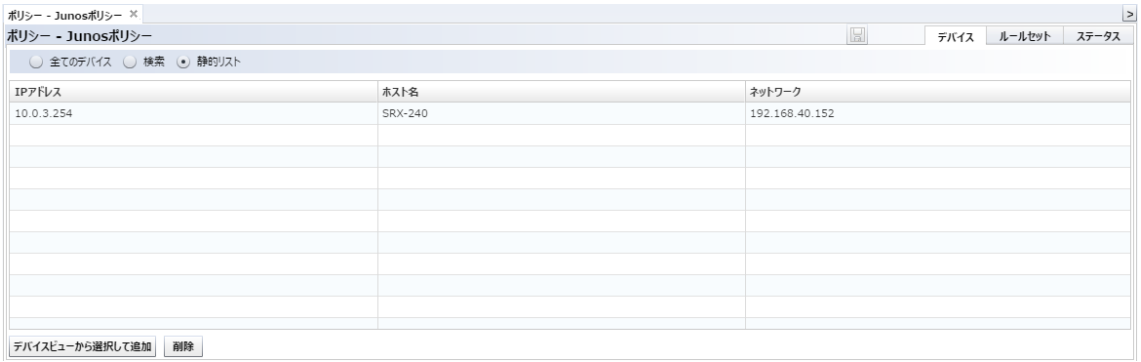
6.15.2 コンプライアンスポリシー

コンプライアンスポリシータブ

コンプライアンスポリシータブは次のサブタブからなります。

デバイスサブタブ

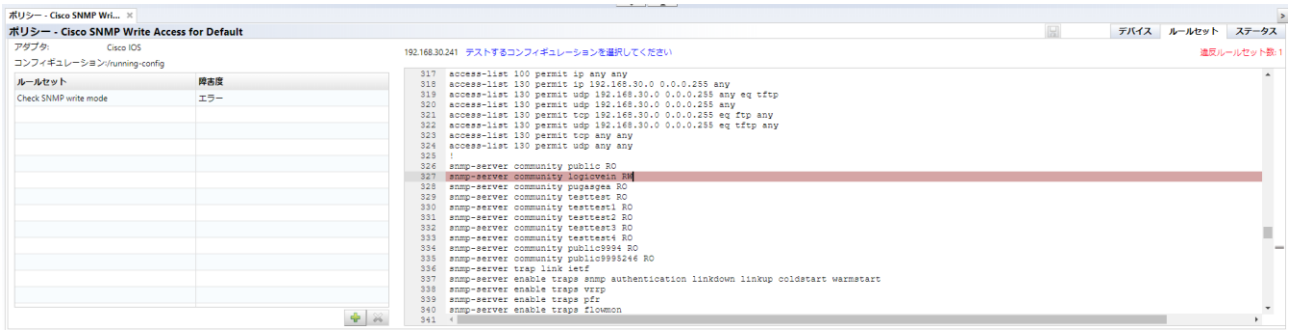
このタブは、ポリシーをどのデバイスに適用するかを選択します。入力インタフェースは、ジョブ管理のものと同じです。静的リスト、検索、すべてのデバイスの 3 つの方法を用い、タブ切り替えテクニックを適宜用いてデバイスを選択します。



項目	説明
全てのデバイス	全てのデバイスにポリシーを適用します。
検索	検索条件に一致したデバイスにポリシーを適用します。
静的リスト	「デバイス」タブで選択して追加したデバイスにポリシーを適用します。(*タブ切り替えテクニック*を使います。)

ルールセットサブタブ

このタブでは、作ったルールセットをポリシーに登録します。



項目	説明
アダプタ	ポリシーを適用するアダプタを表示しています。
コンフィギュレーション	ポリシーを適用するコンフィギュレーションを表示しています。
ルールセット	ポリシーに追加したルールです。
障害度	障害のレベルを、*エラー*または*ワーニング*から選択できます。ポリシー違反時に表示されるアイコンが異なります。

新規ポリシーの作成

先程作成したルールセットを用いて、Cisco IOS デバイスコンフィギュレーション用のポリシーを作成してみましょう。

コンプライアンス→コンプライアンスポリシータブ にて 

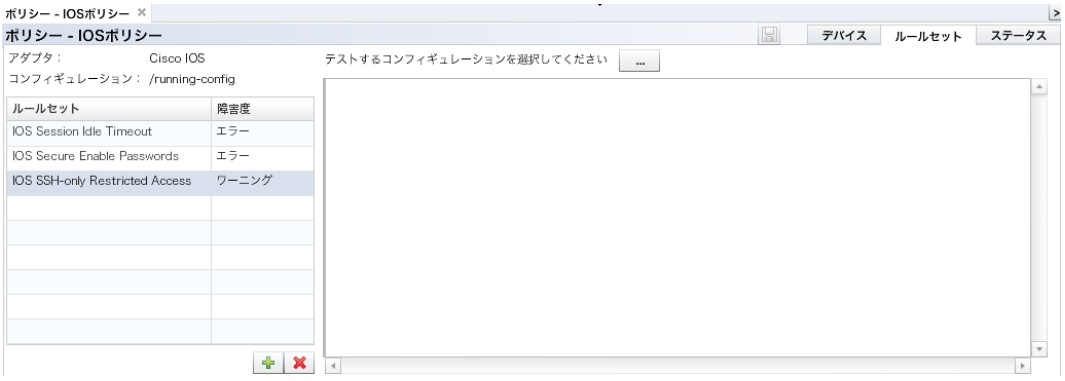
ボタンを押してください。

ポリシー名、対象アダプタ、コンフィギュレーションの種類を入力して OK ボタンを押してください。

デバイスサブタブにて、この例では検索を選択します。例として、ここではモデルフィルタに *Cisco* と入力しましょう。 モデル名に Cisco という文字列を含むデバイスのみが対象になります。

このデバイスサブタブでの検索、静的リストなどの動作と設定方法は、ジョブ管理タブで行う動作・設定方法と全く同じです。結果としてジョブ管理タブで行うのと同様に、検索ルールを用いた時には違反チェックが起動するたびに対象デバイスが検索され、そのデバイスにのみ違反チェックが行われます。ポリシー作成時の検索結果が保存されるわけではない事に注意してください。

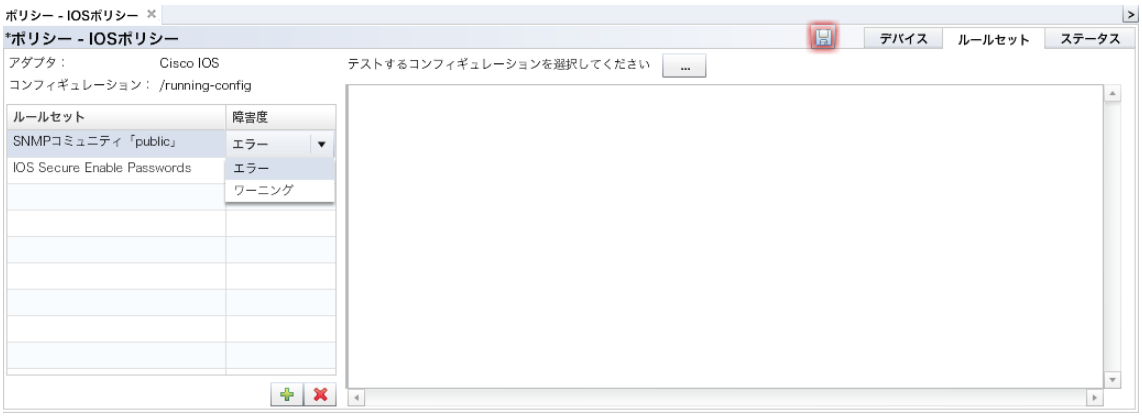
ステータスペインのルールセットサブタブにて、ボタンを押してください。



ルールセットを選択しボタンを押してください。この例では、SNMP コミュニティ「public」& IOS セキュア Enable Password ルールを選択しました。

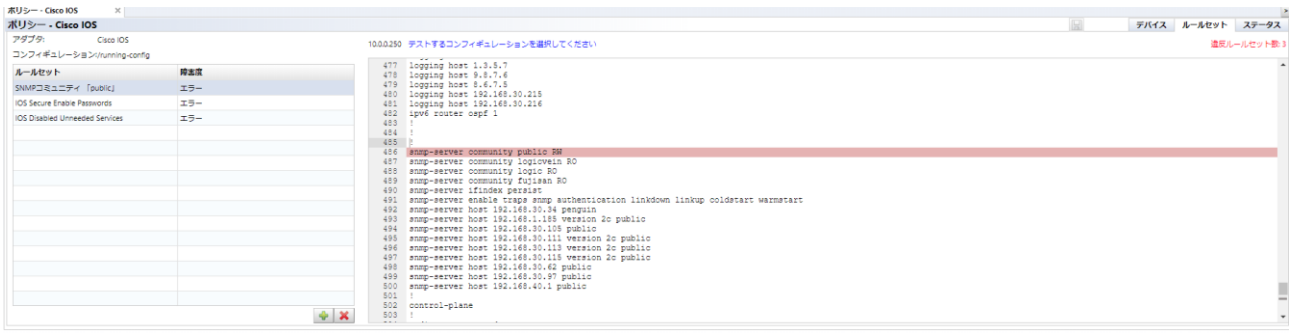
このウィンドウに現れるルールは、そのアダプタタイプが現在のポリシーのアダプタタイプにマッチするものに限られます。 全くルールが表示されない場合には、ポリシーかルールのアダプタタイプを見直してください。

ルールの*障害度*を選択します。ルールセットごとに異なる障害度を設定することができます。



ポリシーをテストするには、テストするコンフィギュレーションを選択してくださいをクリックし、コンフィギュレーションを選択してください。(ルールセットのテストで行った手順と同じです。)

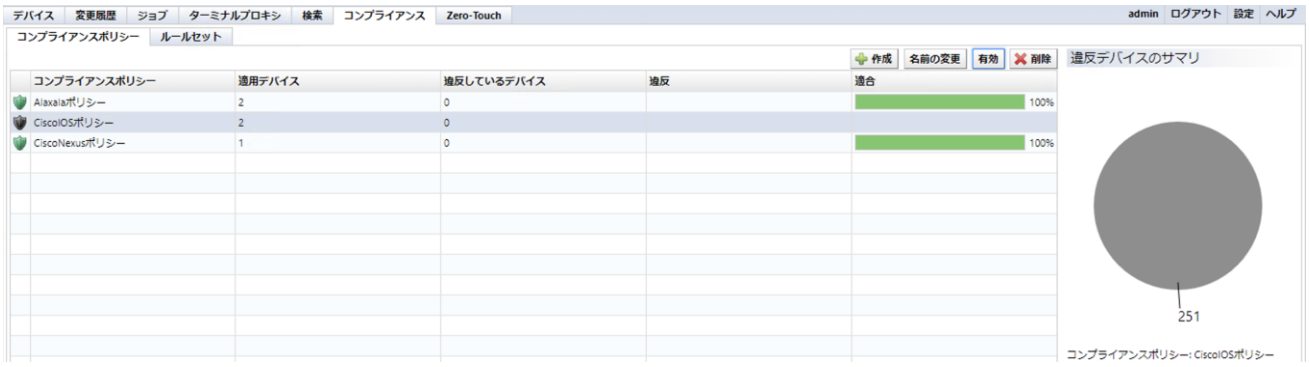
このテストルールに対して違反が検索され、そしてもし違反が見つかれば赤で表示されます。テスト結果を確認したら、次はポリシーを有効化しましょう。ポリシーを作成しただけでは、違反チェックは行われません。



作成したポリシーの適用

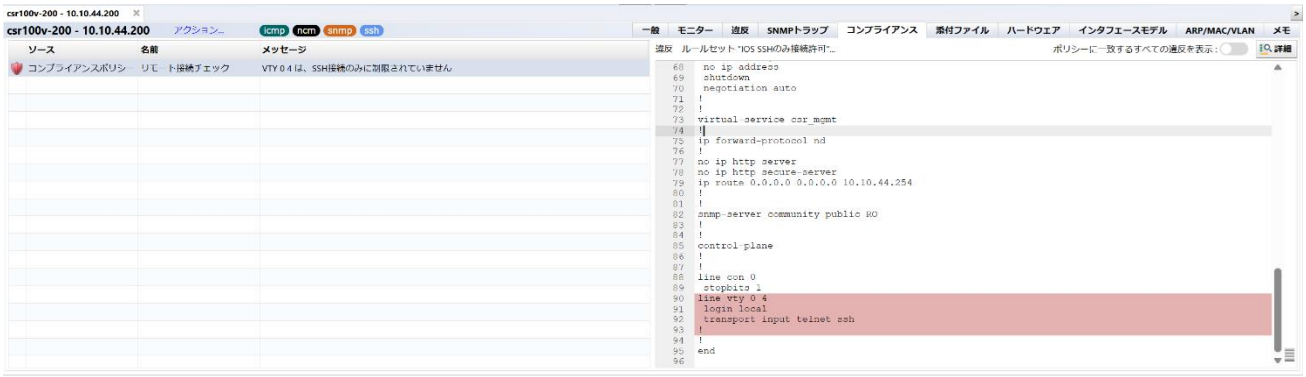
ポリシーを作成したら、次にポリシーを有効化する必要があります。メインペインにコンプライアンス→コンプライアンスポリシーサブタブが開かれていることを確認してください。

ポリシーを選択した状態で有効ボタンを押してください。右の違反デバイスのサマリに円グラフが表示され、違反状況が一目でチェックできます。



ポリシー違反のあるデバイスがあった場合には、ポリシーのアイコンが変化します。その障害度に応じて、オレンジのワーニング、 あるいは赤いエラーアイコンが表示されます。

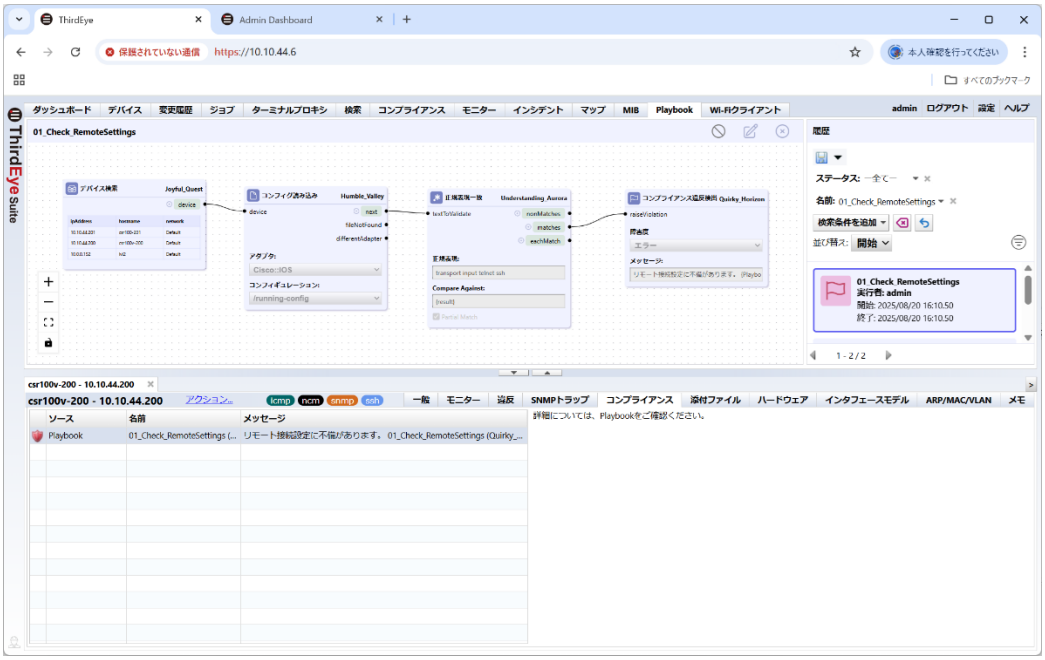
変化したアイコンをダブルクリックしましょう。すると、ステータスペインに*ステータス*サブタブが開かれます。このサブタブには、違反の詳細が書かれています。



違反アイコンはデバイスビューにも表示されます。 アイコンをダブルクリックすれば、違反の詳細を知ることができます。

補足

Playbook の［コンプライアンス違反検知］ノードを使用すると、デバイスビューに違反が登録されます。登録された違反の詳細は、Playbook の履歴から確認できます。



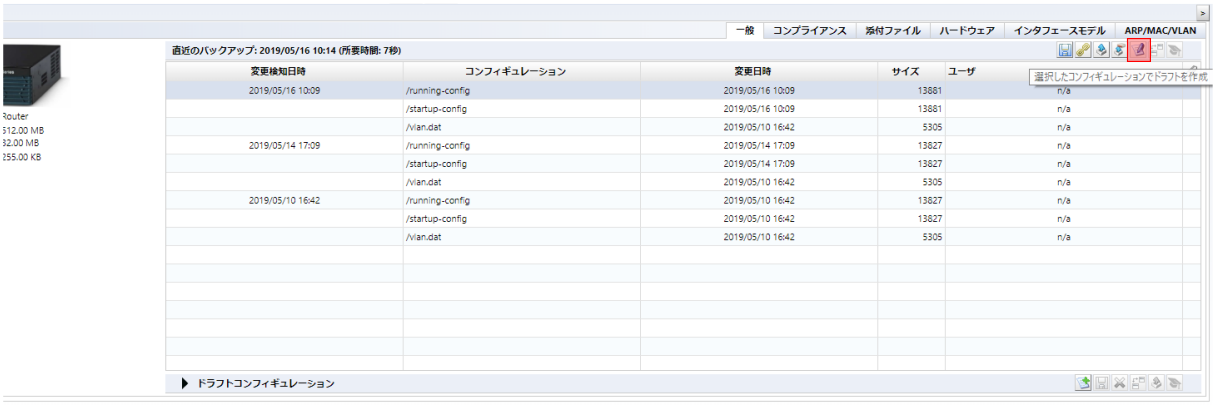
6.16 ドラフトコンフィギュレーション

ドラフトコンフィギュレーションとは、バックアップ履歴と独立に保存されたコンフィギュレーションのことです。その性質はバックアップされた普通のコンフィグ履歴と殆ど同じですが、いくつか追加要素があります。たとえば、それぞれに名前を与えることができ、外部のプレーンテキストに保存すること、およびインポートすることが可能です。この機能は、同じデバイスコンフィギュレーションを何度か再利用する場合に便利です。

6.16.1 ドラフトコンフィギュレーションの作成

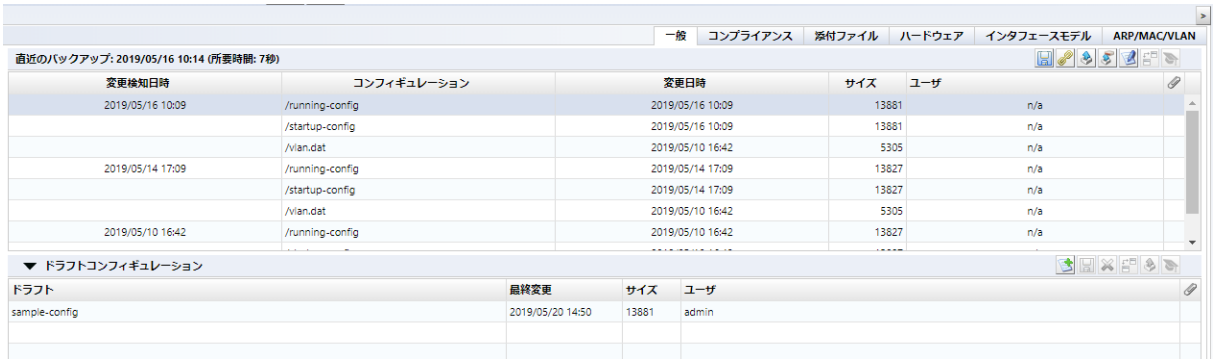
ドラフトコンフィギュレーションは、既存のコンフィギュレーション履歴からコピーして作ることが出来ます。はじめに、対象デバイスをダブルクリックしてコンフィグ履歴を開いてください。

バックアップされたコンフィギュレーションからドラフトコンフィギュレーションのベースとなるものをクリックして選択します。選択した状態で、  ボタンを押します。

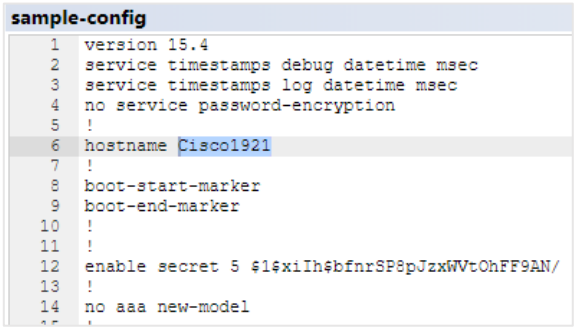


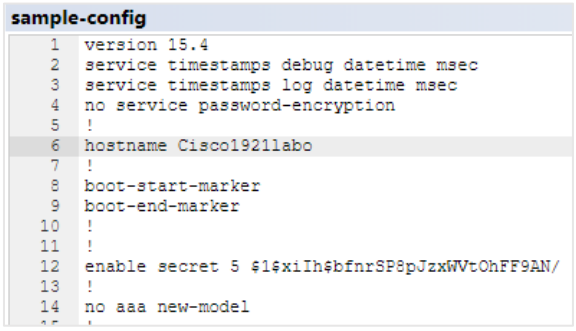
ドラフトコンフィギュレーションの名前を入力し、OK をクリックします。

ドラフトコンフィギュレーションを編集するには、項目をダブルクリックします。



作成されたドラフトコンフィギュレーションをダブルクリックします。編集ウィンドウが開き、コンフィグを直接できるようになります。 編集が完了したら  を押してコンフィグを保存してください。





保存すると、ドラフトコンフィグの変更履歴が同時に保存されます。

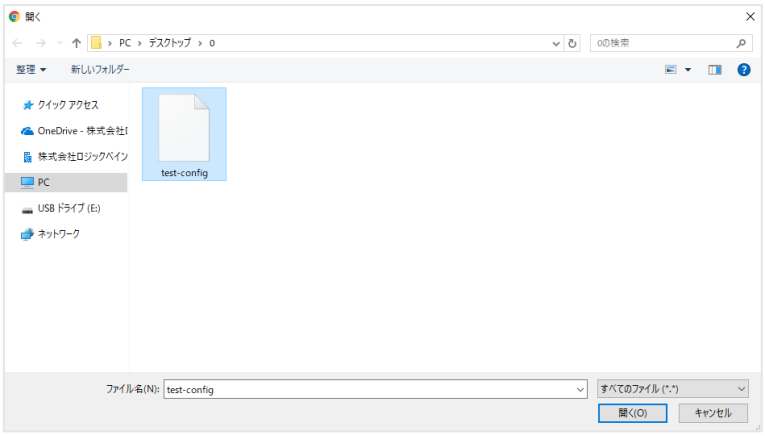
6.16.2　プレーンテキストからドラフトコンフィギュレーションをインポートする

ここでは、外部のテキストファイルからドラフトコンフィギュレーションを作成します。

すでにインポートするテキストファイルが存在しているものとします。まず、デバイスビューで対象デバイスをダブルクリックし、 コンフィグ履歴を表示してください。

ステータスペインで  ボタンを押してください。

インポートするファイルを選択し、「開く」をクリックします。



テキストファイルの内容がインポートされ、 ドラフトコンフィギュレーションが作成されます。

6.16.3　ドラフトをエクスポートする

エクスポートするには  ボタンを押してください。

6.16.4　ドラフトを削除する

削除するには  ボタンを押してください。

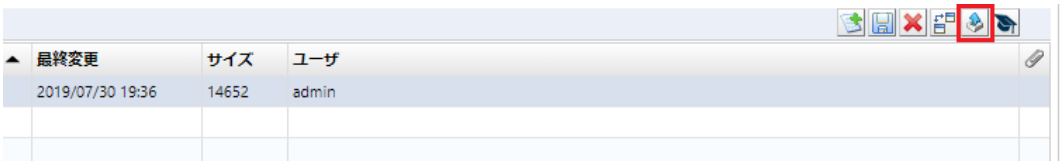
6.16.5　ドラフト同士の比較

コンフィギュレーション同士を比較するには  ボタンを押します。比較において、ドラフトはコンフィグ履歴と同様に扱うことが出来ます。そのため、詳細な方法は「コンフィギュレーションの比較」をご参照ください。

6.16.6　ドラフトコンフィギュレーションをデバイスに適用する

ドラフトの比較と同じく、ドラフトの適用もバックアップコンフィグの適用(復元)と同じ手順で行うことが出来ます。ただし、ただ一点異なる点が生じます。

アップロードするドラフトコンフィギュレーションを選び、  ボタンを押してください。



running-config と startup-config のどちらにアップロードするかを選択してください。この点が履歴のアップロードとの唯一の相違点です。(履歴のアップロードでは、running-config は running-config に、startup-config は startup-config にそれぞれアップロードされます。)

OK を押してアップロードを開始してください。

6.17 チェンジアドバイザ

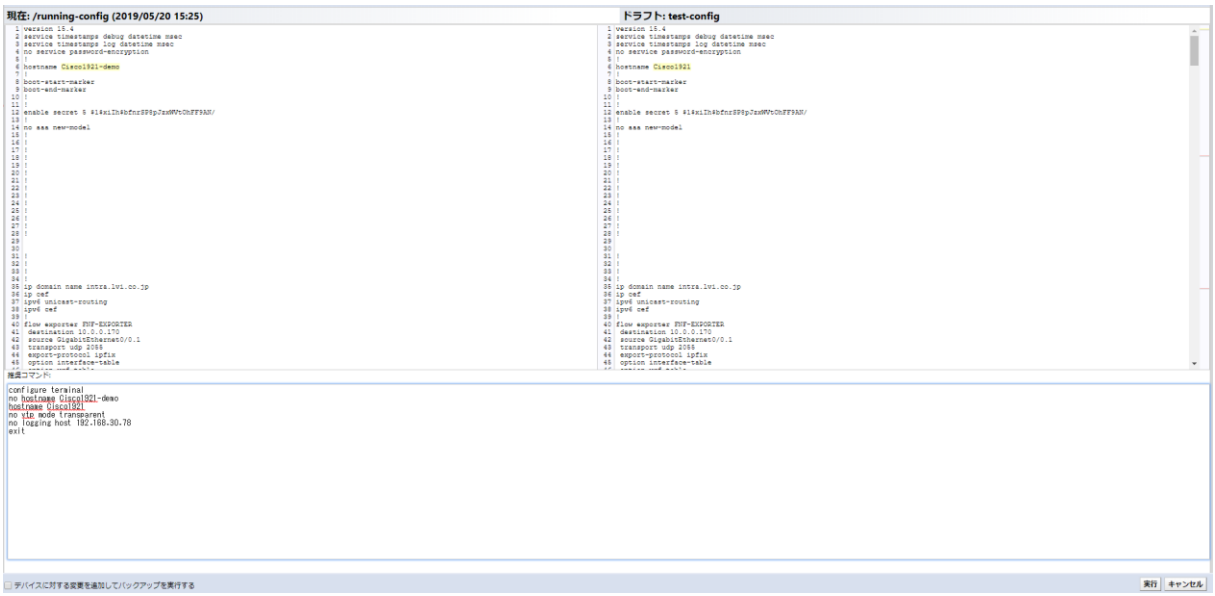
チェンジアドバイザは、現在のコンフィグと指定されたコンフィグを読み込み、前者を後者に変更するために必要な設定変更コマンドを出力してくれる機能です。(この機能は一部デバイスでは使用出来ません。)

デバイスビューでデバイスをダブルクリックしてください。

コンフィギュレーション履歴あるいはドラフトから、コンフィグを選んでください。

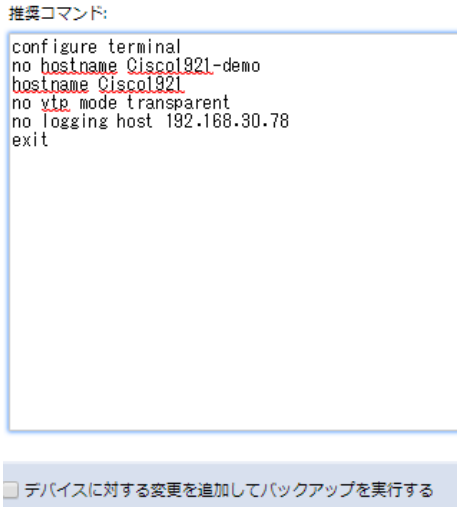
 ボタンを押してください。

チェンジアドバイザが起動し、下側のペインでコマンドが提示されます。

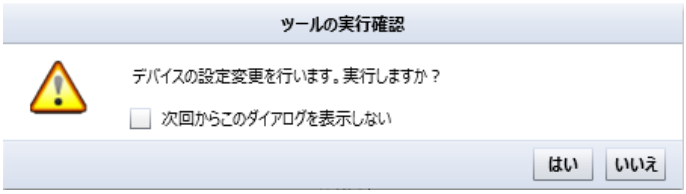


6.17.1　チェンジアドバイザを用いてコマンドを実行する

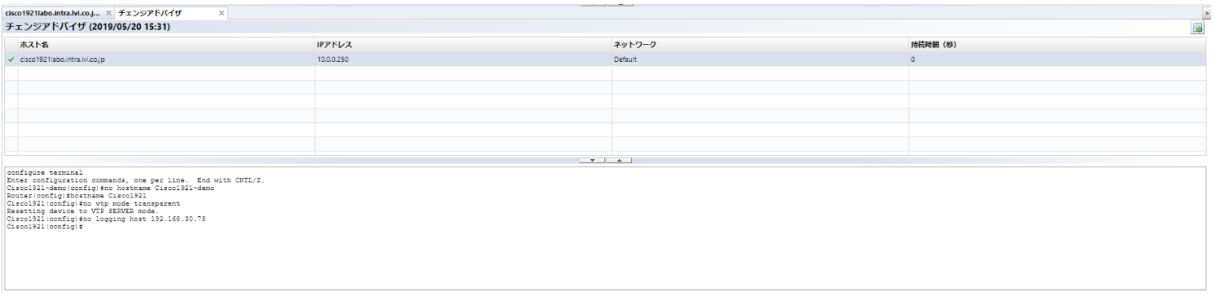
チェンジアドバイザの出力したコマンドをデバイスで実行することが出来ます。提示されたコマンドを実行する前に、実行するコマンドを一度確認してください。不適切なコマンドがあった場合には、出力されたコマンドを直接編集することが出来ます。生成されたコマンドはチェックしましょう。



その後、 実行を押してください。[はい] を押して進みます。



コマンドを実行後、結果を確認することが出来ます。チェンジアドバイザの実行結果・履歴はジョブ履歴にも表示されます。



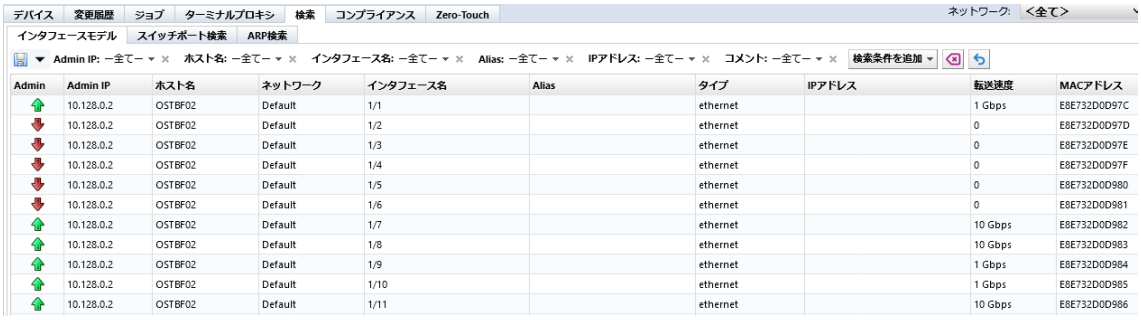
コンフィギュレーションの復元やドラフトコンフィギュレーションのアップロードでは、主な通信プロトコルは TFTP です。したがって、復元およびアップロード機能は TFTP の実装されていないデバイスでは利用不可です。一方、チェンジアドバイザ機能は CLI ログイン(telnet/SSH)さえサポートしていれば利用できます。CLI ログインはほとんどの機種がサポートしておりますので、アップロードが利用不可能な環境でも、チェンジアドバイザの機能を用いて代用することが出来ます。

6.18 検索

この節は、検索タブから利用可能な機能について解説します。これらの機能は、名前は似ていますがデバイスビューでの検索とは全く関係がありません。 検索タブは以下のサブタブから成り立ちます。

6.18.1 インタフェースモデル

インタフェースモデルでは、登録されているデバイスが持つインタフェースを一覧表示します。



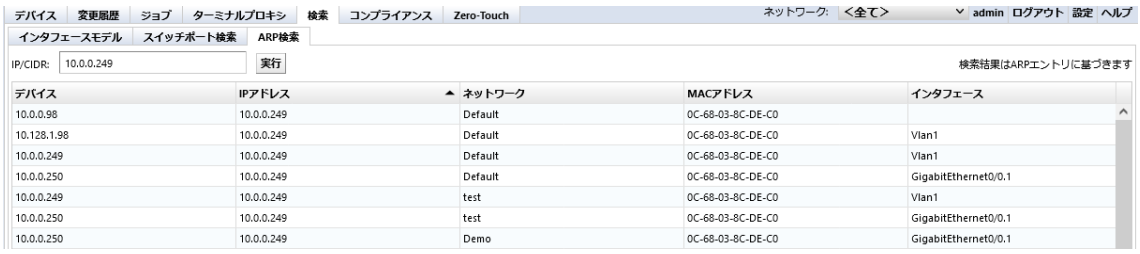
Admin	Admin IP	ホスト名	ネットワーク	インタフェース名	Alias	タイプ	IPアドレス	転送速度	MACアドレス
↑	10.128.0.2	OSTBF02	Default	1/1		ethernet		1 Gbps	E8E732D0D97C
↓	10.128.0.2	OSTBF02	Default	1/2		ethernet		0	E8E732D0D97D
↓	10.128.0.2	OSTBF02	Default	1/3		ethernet		0	E8E732D0D97E
↓	10.128.0.2	OSTBF02	Default	1/4		ethernet		0	E8E732D0D97F
↓	10.128.0.2	OSTBF02	Default	1/5		ethernet		0	E8E732D0D980
↓	10.128.0.2	OSTBF02	Default	1/6		ethernet		0	E8E732D0D981
↑	10.128.0.2	OSTBF02	Default	1/7		ethernet		10 Gbps	E8E732D0D982
↑	10.128.0.2	OSTBF02	Default	1/8		ethernet		10 Gbps	E8E732D0D983
↑	10.128.0.2	OSTBF02	Default	1/9		ethernet		1 Gbps	E8E732D0D984
↑	10.128.0.2	OSTBF02	Default	1/10		ethernet		1 Gbps	E8E732D0D985
↑	10.128.0.2	OSTBF02	Default	1/11		ethernet		10 Gbps	E8E732D0D986

6.18.2 スイッチポート検索

スイッチポート検索はネットワーク中のデバイスを FQDN (Fully Qualified Domain Name)、 IP アドレスあるいは MAC アドレスを用いて検索することが出来ます。検索結果として表示されるのは、ネットワークノードの ARP および NDP、あるいはスイッチポートの情報です。下の画面は、IP アドレス 10.0.0.249 を指定した際の検索結果です。

6.18.3 ARP 検索

ARP 検索タブでは、管理ノードの IP アドレスを指定して検索し、ARP 情報を表示します。下の画面は、IP アドレス 10.0.0.249 を指定した際の検索結果です。



デバイス	IPアドレス	ネットワーク	MACアドレス	インタフェース
10.0.0.98	10.0.0.249	Default	0C-68-03-8C-DE-C0	
10.128.1.98	10.0.0.249	Default	0C-68-03-8C-DE-C0	Vlan1
10.0.0.249	10.0.0.249	Default	0C-68-03-8C-DE-C0	Vlan1
10.0.0.250	10.0.0.249	Default	0C-68-03-8C-DE-C0	GigabitEthernet0/0.1
10.0.0.249	10.0.0.249	test	0C-68-03-8C-DE-C0	Vlan1
10.0.0.250	10.0.0.249	test	0C-68-03-8C-DE-C0	GigabitEthernet0/0.1
10.0.0.250	10.0.0.249	Demo	0C-68-03-8C-DE-C0	GigabitEthernet0/0.1

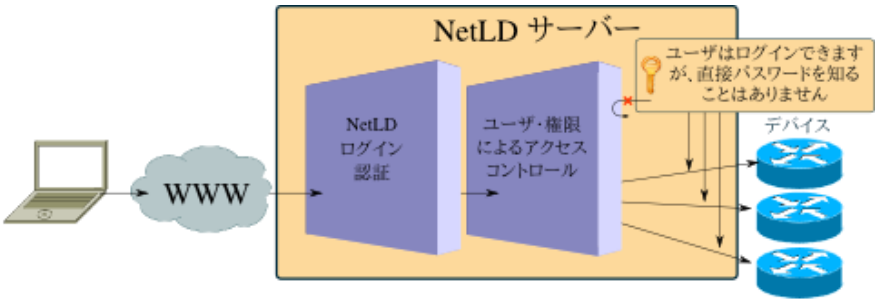
7. 発展ツール

この章では、大規模ネットワーク・リモートネットワークを管理するために必要なツール群を解説します。これらのツールを用いることで、実務で用いているネットワークの可用性を高く維持しながら、管理コストを低く保つことができます。

7.1 ターミナルプロキシ

ターミナルプロキシ機能は、管理されているデバイスへ netLD 経由で接続できるようになる機能です。接続は、まず netLD サーバに接続し、これを踏み台として対象のデバイスに接続するという形を取ります。ターミナルプロキシを用いる利点は、ログインに際してデバイスのログインパスワードをいちいち入力する必要がないという点が挙げられます。netLD サーバが代わりに入力を行うようになっています。もうひとつの利点は、ターミナル上での操作がすべてログに自動的に記録されることです。これは、後で問題の原因を解明するのに役に立ちます。

さらなる応用方法として、これらの利点をうまく活かし、ネットワーク管理を安全に外部委託するという手法があります。もし netLD なしでデバイスの管理を外部の人間に委託する場合、その外部の人間に設定変更を行わせるためには、デバイスのログインパスワードを直接外部の人間に伝える必要があります。しかし、このことは、直接のログインパスワードが外部に流出する可能性を示します(パスワードが盗まれ、不正な人間が外からデバイスにアクセスする可能性があります)。 このとき、不正な人間が行った操作ログや、誰が流出元になったのかの情報を得ることはできません。一方で、ターミナルプロキシを用いると、ネットワークの所有者は *デバイスのパスワードではなく* netLD ユーザアカウントのログインパスワードを通知するだけで済みパスワード情報の漏洩を心配する必要がありません。netLD のユーザアカウントは、操作ごとにユーザと権限の概要で見たような権限を設定でき、またターミナルプロキシの機能によりログがすべて記録されるので、より安全です。



以降の章では、ターミナルプロキシ機能を有効化するための手順を説明します。

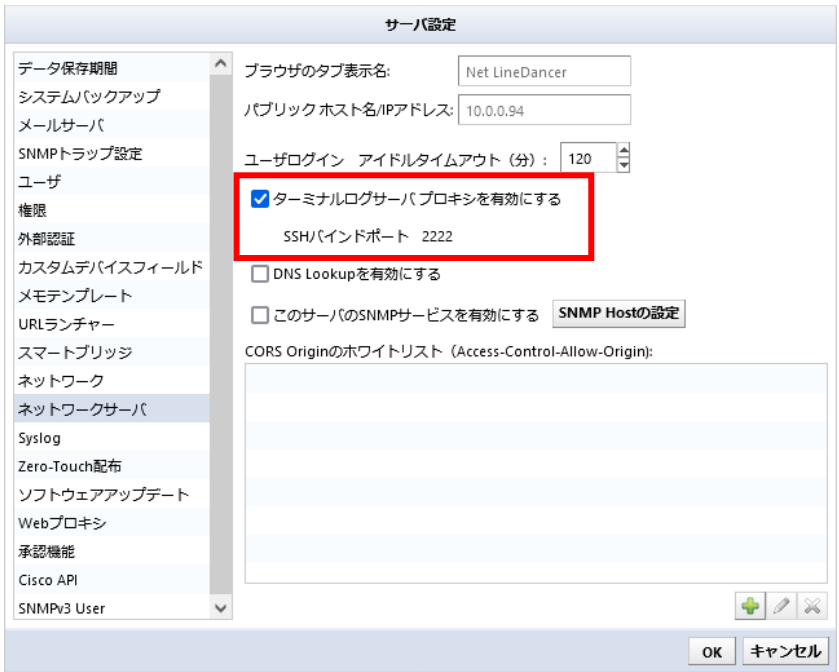
7.1.1 使用可能なコマンド

ターミナルプロキシでは以下のコマンドが使用可能です。

コマンド	説明
connect {IP アドレス または ホスト名}	デバイスに SSH か telnet で接続します(両者ともインベントリ/クレデンシャルの設定が必要です)。
connect {initials}	インベントリ内の名前が与えられた頭文字で始まるデバイスを、最大 20 個表示します。
device {IP アドレス または ホスト名}	指定されたデバイスの詳細情報を表示します。
device {ホスト名}	上の connect コマンドと同様に、候補となるデバイスを最大 20 個表示します。
exit	netLD との SSH 接続を切断します。
help	コマンドのリストを表示します。
network {ネットワーク}	ネットワークを設定します。
version	netLD のバージョンを表示します。

7.1.2 ターミナルプロキシを有効にする

この機能はデフォルトで有効になっています。機能の有効・無効を切り替えるためには、設定ウィンドウから設定→ネットワークサーバ と進み、ターミナルログサーバプロキシを有効にするチェックボックスを切り替えてください。設定が終了したら、OK ボタンを押して設定を保存してください。ファイアウォールを有効にしている場合には、ファイアウォールを適切に設定し、SSH アクセスを許可してください。設定が適切でないと、接続が失敗してしまいます。



7.1.3 ログイン

ターミナルプロキシ機能を有効化したら、ログインを試してみましょう。ログイン前に、netLD サーバの IP アドレスを覚えておいてください。

まず、お好きな SSH クライアントで netLD サーバに接続してください。クライアントの指定はありません。Unix 上の OpenSSH でも、Windows では Tera Term などを用いることも可能です。以下の例では、サーバが IP アドレス 192.168.0.77 にあり、クライアントが bash から OpenSSH を用いて接続する場合を説明します。もう一度念を押しますが、ファイアウォールが有効なネットワークで netLD サーバに接続するためには、ファイアウォールを適切に設定し、SSH ポートへのアクセスを許可してください。

```
bash>
```

netLD サーバに、ssh を用いて普通にログインしてください。ユーザ名とパスワードは、GUI でのログインの際に求められるものと同じ物を使うことができます。SSH の使用するポートはデフォルトで 22 ですが、VA 版 netLD のターミナルプロキシ用受付ポートは 2222 番に固定してありますので、接続の際に-p2222 のようにポートを指定することを忘れないでください。

```
bash> ssh admin@192.168.0.77 -p 2222
admin@192.168.0.77's password:
Active network: Default
Welcome to Net LineDancer - 2014/03/26 11:33:20 JST
netld#
```

netLD サーバへの接続はこれだけで完了です。続いて、サーバを経由して、管理下のデバイスにログインを行なってみましょう。デバイス・シェルへのログインは、connect {IP アドレス または ホスト名} によって行うことができます。

```
netld# connect 10.0.0.2
connect 10.0.0.2
Resolving device 10.0.0.2...
Connecting to device 10.0.0.2...

Warning: skipping login authentication until
an administrative user is added.

NEC Portable Internetwork Core Operating System Software
Copyright Notices:
Copyright (c) NEC Corporation 2001-2010。 All rights reserved.
Copyright (c) 1985-1998 OpenROUTE Networks, Inc.
Copyright (c) 1984-1987, 1989 J. Noel Chiappa.
IX2025_LVI# enable-config
```

```
Enter configuration commands, one per line. End with CNTL/Z.
IX2025_LVI(config)#
```

この際、デバイスへは管理者権限でログインすることになり、またログイン直後から自動で enable 状態になっています。（ただし、クレデンシャルにて enable パスワードが適切に設定されている場合。）ここでは、通常デバイス上のログインシェルで行うことのできる全ての操作を行うことができ、またその操作は netLD に記録されています。このとき、GUI から netLD にログインしている他のユーザは、ターミナルプロキシタブからあなたがログインして何か操作を行なったことを操作直後にリアルタイムで見ることができます(後述)。

注:ネットワークを変更する場合、自分のユーザがそのネットワークを閲覧・操作する権限を持っていることを確認してください。権限が与えられていない場合、あなたがログインできるネットワークは Default ネットワークだけになります。ネットワークの変更は network<ネットワーク名>で行うことができます。

作業が終わったら、exit コマンドを数回打ち込んで、netLD の SSH セッションまで戻ってください。

```
IX2025_LVI(config)# exit
exit
IX2025_LVI# exit
exit
Connection to 10.0.0.2 closed.
netld#
```

この例では、はじめの一回は enable 状態からの脱出、二回目はデバイスのログインシェルからの脱出です。操作はデバイスごとに異なります。ログアウトを行う際、netLD はデバイスのバックアップを自動で取ります。また、デバイスの設定が変更されていた場合、その変更はコンフィギュレーション履歴に保存されます。

さらにもう一度 exit を打つことで、netLD との SSH 接続を切断することができます。

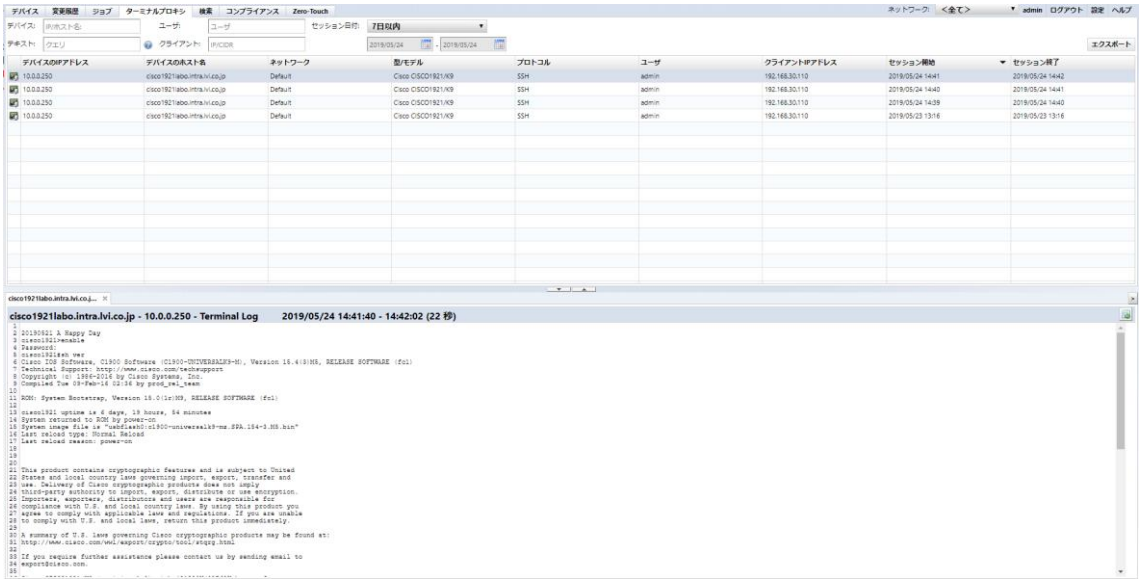
```
netld# exit
exit
Connection to 192.168.0.77 closed.
bash>
```

7.1.4 自動補完

netLD サーバとの接続中、コマンド(例えば connect c)は名前が c で始まるデバイスのリストを表示します。 このとき、リストの数字を入力して Enter を打つと、対応するデバイスにログインが行われます。その他にも、例えば connect c<Tab>を入力すると、同様に c で始まるデバイスのリストが表示されます。リストの中に想像していたデバイスが見つからない場合には、さらに文字を追加することでリストを絞り込んでいくことが可能です。先程の例で例えば cisco <Tab> というのを追加入力すれば、リストの中の候補は cisco という文字列を含むものだけが表示されるようになります。

7.1.5 ターミナルプロキシログ

ターミナルプロキシ上で行われた操作の履歴は、ターミナルプロキシタブで後に確認することができます。ターミナルプロキシタブを開くと、ログが表に一覧になって表示されています。ログの一つをダブルクリックすると、ステータスペインにて詳細情報を見ることができます。



項目	説明
デバイスの IP アドレス	該当セッションで接続したデバイスの IP アドレス
デバイスのホスト名	同 ホスト名
型/モデル	同 型/モデル
プロトコル	ログインに用いられたプロトコル
ユーザ	ログインしたユーザ名(netLD ユーザアカウント名)
クライアント IP アドレス	netLD にログインした端末の IP アドレス
セッション開始	セッション開始時刻
セッション終了	セッション終了時刻

ターミナルログには検索をかけることができます。 検索は 5 通りの方法があります。

項目	説明
デバイス	ログインに用いた IP アドレスとホスト名
Text	入力されたコマンドラインへの検索
ユーザ	netLD 上でのログインユーザ名
クライアント	netLD にログインした端末の IP アドレス
セッション日付	ログインが行われた日付を限定

デバイスビューでデバイスを右クリックすると、現れるメニューに*ターミナルログ表示*という項目があります。これは、デバイスごとの履歴を簡単に見ることのできるショートカットになっています。

7.1.6 変更履歴を通してログをチェックする

ターミナルプロキシ上の操作の結果自動でバックアップが行われた場合、このバックアップも、普通のバックアップと同様に、バックアップ履歴(設定変更履歴)の中に表示され、いつバックアップが行われたかを確認することができます。対象となる設定を選択した状態で  ボタンをクリックすれば、対応するチェンジサマリ・サブタブがステータスペインに表示されます。

対象となる設定を選択した状態で  ボタンをクリックします。

対応するチェンジサマリ・サブタブがステータスペインに表示されます。

7.1.7 ログファイルのエクスポート

メインペインのターミナルプロキシタブで Export ボタンをクリックすると、フォルダ選択ウィンドウが現れ、ログファイルが指定したフォルダに zip 形式で保存されます。

アーカイブ内は以下のようなディレクトリ構成を持ちます。

<filename>.zip
<network name>
10.0.0.1(1812J-B)
10.0.0.201(cisco2500b.intra.dar.co.jp)
10.0.0.203 (cisco2600a.intra.dar.co.jp)
10.0.0.208 (C2801)
…

7.2 Zero-Touch（オプション）

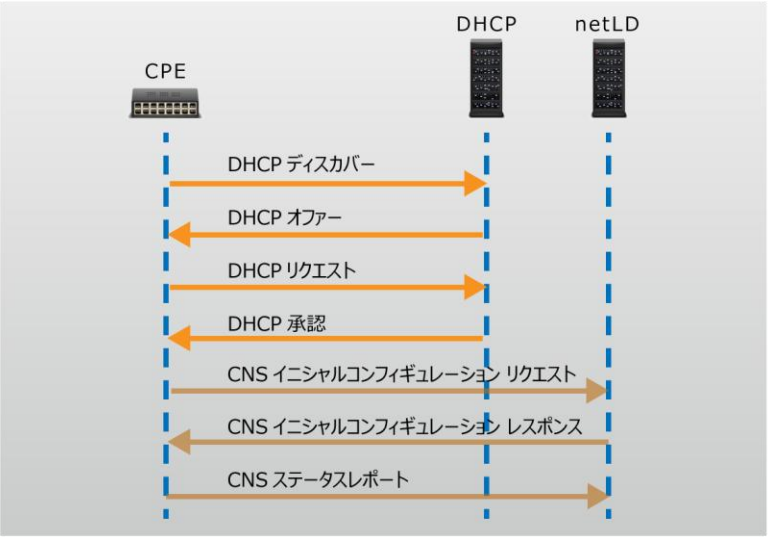
Zero-Touch は、物理的に離れたネットワーク上のデバイスにコンフィギュレーションを配布するのに便利なツールです。ツールは Cisco Plug and Play や Cisco Networking Services (CNS)の機能を背景としているので、Zero-Touch はそれらの機能に対応したデバイスでしか用いることができません。

Zero-Touch がコンフィグを配布する形式は主に 3 つあります。

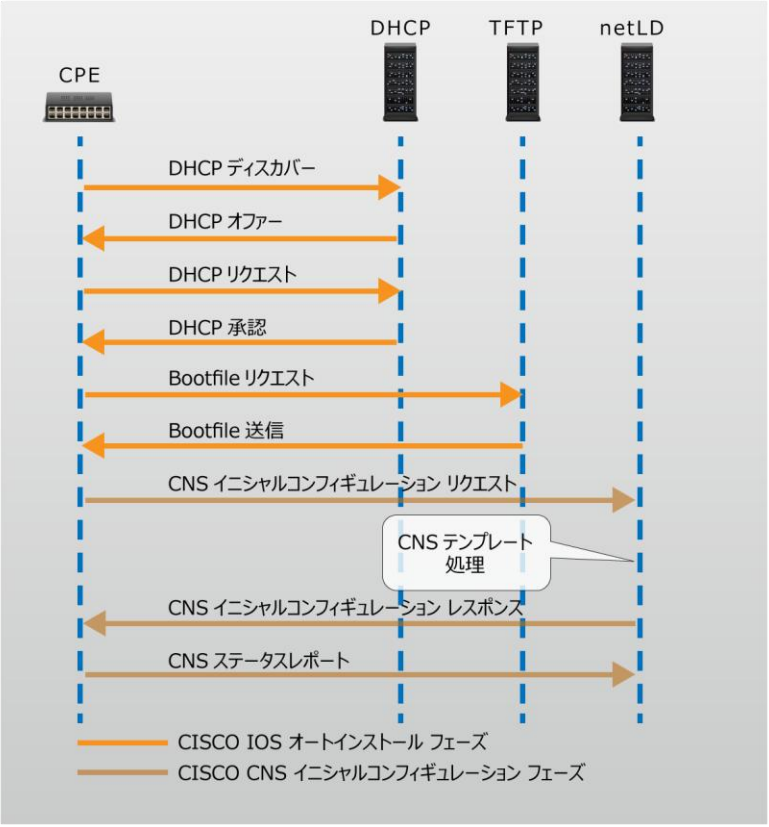
1. テンプレート：テンプレートベースでコンフィグを配布します。リモートオフィスに新たなデバイスをネットワークに導入する場合に使います。
2. セルフリカバリ：異常コンフィグを上書きされてしまい、うまく動かなくなってしまったデバイスをリセットするのに便利です。
3. 特定デバイスの復元：デバイス装置の更新に便利です。例えば、今まで使われていたデバイスが故障し、同じモデルの別のデバイスに入れ替える場合、それまで使われていた設定を新たなデバイスに書きこむことができます。

Zero-Touch は、以下のようなプロトコルを用いてコンフィギュレーションを配布します。したがって、使用の際にはファイアウォールを適切に設定することが必要となります。

下の図は、PnP を使用した Plug and Play が行う処理の流れを示しています。 図を見やすくするために、DHCP, netLD サーバを分割して示して有りますが、これは、3 つのコンピュータを用いるわけではありません。 3 つのサーバプログラムはすべて、netLD サーバの動いている一台のコンピュータ上で実行されます。



下の図は、CNS を使用した *Plug and Play* が行う処理の流れを示しています。PnP を使用した場合と違い DHCP で IP アドレスを取得後、TFTP で Bootfile を取得します。

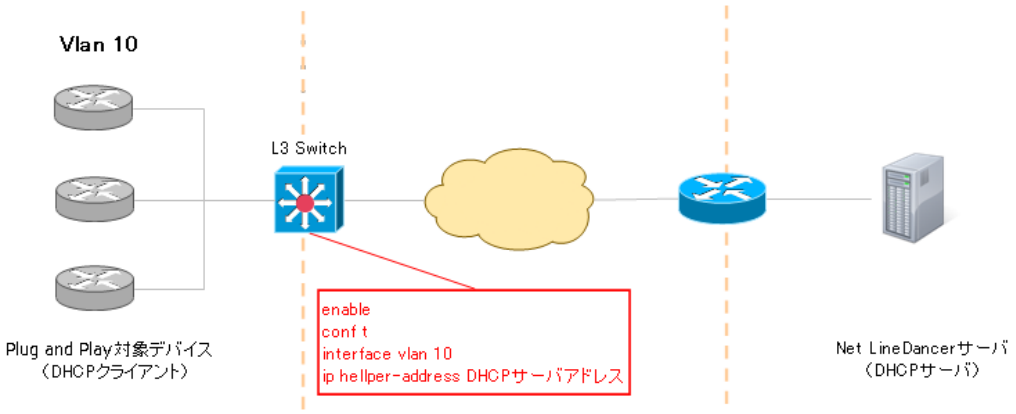


7.2.1 Zero-Touch 要求条件

Zero-Touch を用いるには、以下の条件が整っている必要があります。ご使用の前にご確認ください。

- 対象デバイスの IOS のバージョンは、CNS は IOS 12.2 以降、PnP は IOS 15.2(2)以降である必要があります。
- デバイスは startup-config を持っていてはいけません。
- DHCP サーバ - DHCP サーバを netLD 自身に行わせる場合、対象となるデバイスは DHCP の IP アドレス配布が可能なネットワーク内に存在している必要があります。また、対象デバイスが netLD の配布できるネットワークの外に存在している場合は、経路上にあるデバイスに *DHCP relay* を設定すれば、対象デバイスからの DHCP リクエストを netLD サーバが受信できるようになります。

DHCP リレーの例



7.2.2 Zero-Touch タイプの選択

Zero-Touch のタイプとして Plug and Play と Cisco CNS があります。同時に使用することはできないため、設定→Zero-Touch 配布と進みます。

これが設定ウィンドウの Zero-Touch セクションです。PnP タイプを選択してください。

7.2.3 DHCP サーバ

設定ウィンドウを開き、Zero-Touch セクションにて必要な情報を入力してください。

新たな DHCP プールを設定するには  を押してください。

項目	説明
DHCP サーバを有効にする	netLD がもつ DHCP サーバを利用する場合にはチェックを入れてください。
リース時間	DHCP のリース時間を設定します。

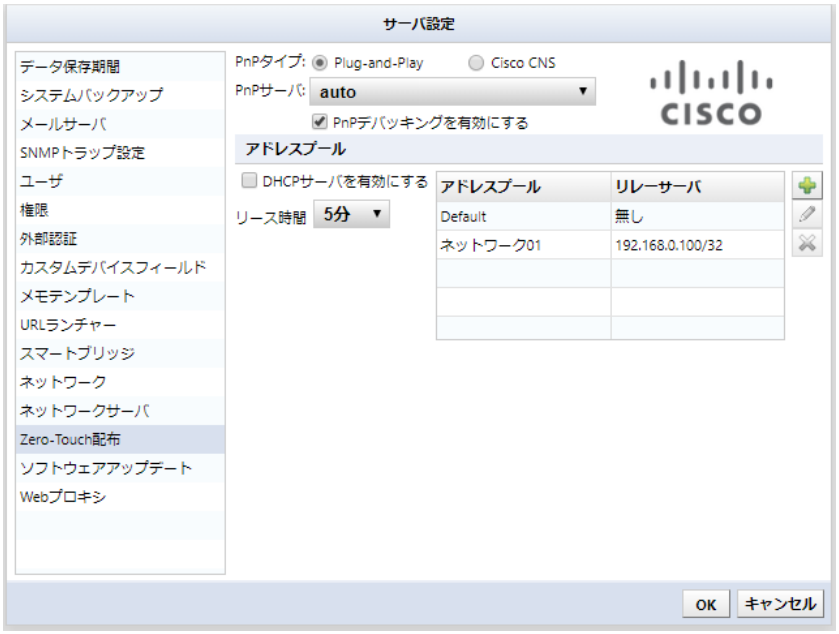
必要な情報を入力し、OK ボタンを押してください。

項目	説明
プール名	作成する DHCP プールの名前を入力
リレーサーバ CIDR	DHCP リレーサーバの存在する IP 範囲を入力
アドレス範囲	配布する IP アドレス範囲を入力(必須)
サブネットマスク	サブネットマスクを入力(必須)
デフォルトゲートウェイ	デバイスのデフォルトゲートウェイを指定

項目	説明
DNS サーバ(オプション)	デバイスからサーバの名前解決を行なうための DNS サーバを指定

入力が完了しました。

正しく操作すれば、下の表に新たな項目が追加されるはずです。



外部の DHCP サーバを使用する

netLD 以外の DHCP サーバを使用する場合には、netLD と通信できる基本的な情報に加え特定のオプションを追加する必要があります。追加するオプションは PnP のタイプにより異なります。

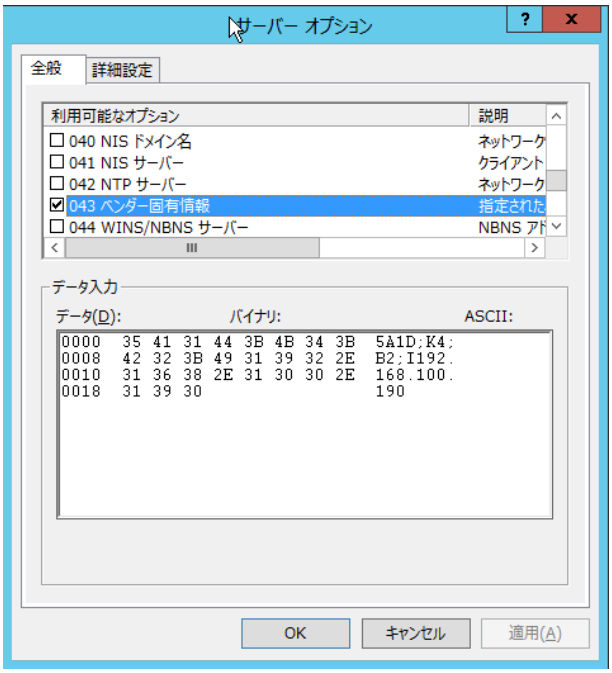
- CNS

オプション 150 またはオプション 6 と 66 どちらも TFTP サーバの情報を渡すオプションです。150 では TFTP サーバの IP アドレスを追加できます。66 では TFTP サーバの名前を追加し 6 で DNS サーバの IP アドレスを追加してデバイスへ渡します。TFTP サーバは netLD を指定する必要があります。Plug and Play が自動で行う処理の流れを示しています。 PnP を使用した場合と違い DHCP で IP アドレスを取得後、TFTP で Bootfile を取得します。

- Plug and Play

オプション 43 オプション 43 では、ベンター固有の情報を追加することができます。

以下の図は Windows の DHCP サーバの設定例です。ASCII 欄に情報を「;」で区切って入力します。



7.2.4　コンフィギュレーションの配布

7.2.4.1　テンプレート

(1)　テンプレートの作成

大きなネットワークでは、似たようなコンフィグをもつデバイスが沢山あることがよく有ります。つまり、コンフィグの違いが IP アドレス、ホスト名、DNS、syslog サーバのアドレスだけであるような場合です。バルクチェンジでは、似たようなコマンドをデバイスごとに柔軟に変化させて送信するための *テンプレート*という方法を用いましたが、Zero-Touch では同じ *テンプレート*をコマンドではなくコンフィグにも使うことが出来ます。

このテンプレートの使い方はすでに解説しているので、ここではその詳細については触れません。もしもその章をまだ読んでいない場合は、テンプレートの考え方についてよく理解するためにも、該当する章をお読みになられることを強く推奨いたします。詳しくは、6.12.4.6 代替値の使用

多くのノードは主な結果とともにメタデータを出力します。「コマンド実行」ノードの場合、device や status などが含まれます。これらはすべて、Playbook の実行開始後にそのノードの出力テーブルで確認できます。フィールドが代替値に対応している場合、値を{中括弧}で囲むことでその値を参照できます。多くのノードでは、これらの値に対してテンプレート化された代替値をサポートしています。

ノード	設定可能フィールド
正規表現一致	正規表現と Compare Against で代替値を設定する事ができます。
コマンド実行	コマンドエディタで代替値を設定する事ができます。
コマンド実行(自動リトライつき)	コマンドエディタで代替値を設定する事ができます。
SSH 実行	コマンドで代替値を設定する事ができます。
変数の設定	値で代替値を設定する事ができます。
フィールド編集	カスタムフィールドで代替値を設定する事ができます。
ファイルアップロード	サーバからファイルを取得するコマンドで代替値を設定することができます。
コンプライアンス違反検出	メッセージで代替を設定する事ができます。

ある情報を独自のメタデータとして抽出し、ノードから列として出力したい場合、最も簡単な方法は「正規表現一致」ノードを使用することです。このノードは Java 形式の正規表現をサポートしており、名前付きマッチグループはその名前を持つ値として取り出されます。例えば Cisco デバイスの稼働時間を「uptime」という名前の値として抽出するには、`show version` コマンドの出力を、以下の正規表現を指定した正規表現一致ノードに渡します。

lab-router uptime is (?[¥w ,]+)

「Compare Against」がデフォルトの {result} に設定されている場合、この正規表現は「Compare Against」の値全体と一致するように設計されません。「Partial Match」を有効にして、正規表現の一部が少なくとも含まれていれば一致としてカウントするように指定しましょう。この設定を行うと、正規表現の一致結果には、一致した uptime が新しい「uptime」列に表示され、後続のノードで {uptime} として使用できます。

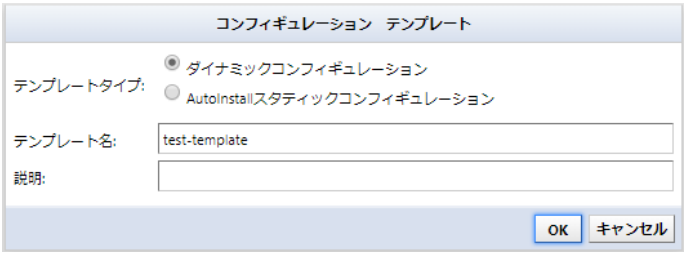
また、「Compare Against」を変更することで、これらを連鎖させてより具体的な情報を取得することも可能です。例えば、最近リセットされたスイッチを確認したい場合は、正規表現の一致条件に「day」を含めない稼働時間を確認することができます。「uptime」の正規表現マッチノードを新しい正規表現マッチノードに接続し、正規表現を day に設定します。「Compare Against」を{uptime}に設定し、「Partial Match」を有効にします。

その後、nonMatches の出力を確認するか、このノードを「Email」、「Webhook」、「コンプライアンス違反検出」、または「変数の設定」ノードに接続し、「デバイスが最近リセットされました：{uptime}」といったメッセージを設定することで、別の方法で結果を受け取ることができます。

バルクチェンジを参照してください。

テンプレートを作るためには以下の手順に従ってください。

Zero-Touch→テンプレートタブに移動し、  を押してテンプレートを作成します。



テンプレートタイプにダイナミックコンフィギュレーションを選び、また新たに作るテンプレートの名前をテンプレート名フィールドに入力します。任意で、説明フィールドを記述することができます。終わったら、OK ボタンを押してください。

画面右に大きなテキストエリアが現れます。元となるコンフィギュレーションを、このエリアに入力して下さい。もし Zero-Touch を行う予定のデバイスと同じ機種のデバイスがインベントリにすでにあるなら、そのデバイスのコンフィギュレーション(例えば start-up config)をコピーし、ここにペーストするのが簡単です。

その後の操作は 6.12.4.6 代替値の使用

多くのノードは主な結果とともにメタデータを出力します。「コマンド実行」ノードの場合、device や status などが含まれます。これらはすべて、Playbook の実行開始後にそのノードの出力テーブルで確認できます。フィールドが代替値に対応している場合、値を{中括弧}で囲むことでその値を参照できます。多くのノードでは、これらの値に対してテンプレート化された代替値をサポートしています。

ノード	設定可能フィールド
正規表現一致	正規表現と Compare Against で代替値を設定する事ができます。
コマンド実行	コマンドエディタで代替値を設定する事ができます。
コマンド実行(自動リトライつき)	コマンドエディタで代替値を設定する事ができます。
SSH 実行	コマンドで代替値を設定する事ができます。
変数の設定	値で代替値を設定する事ができます。
フィールド編集	カスタムフィールドで代替値を設定する事ができます。
ファイルアップロード	サーバからファイルを取得するコマンドで代替値を設定することができます。
コンプライアンス違反検出	メッセージで代替を設定する事ができます。

ある情報を独自のメタデータとして抽出し、ノードから列として出力したい場合、最も簡単な方法は「正規表現一致」ノードを使用することです。このノードは Java 形式の正規表現をサポートしており、名前付きマッチグループはその名前を持つ値として取り出されます。例えば Cisco デバイスの稼働時間を「uptime」という名前の値として抽出するには、`show version` コマンドの出力を、以下の正規表現を指定した正規表現一致ノードに渡します。

lab-router uptime is (?[¥w ,]+)

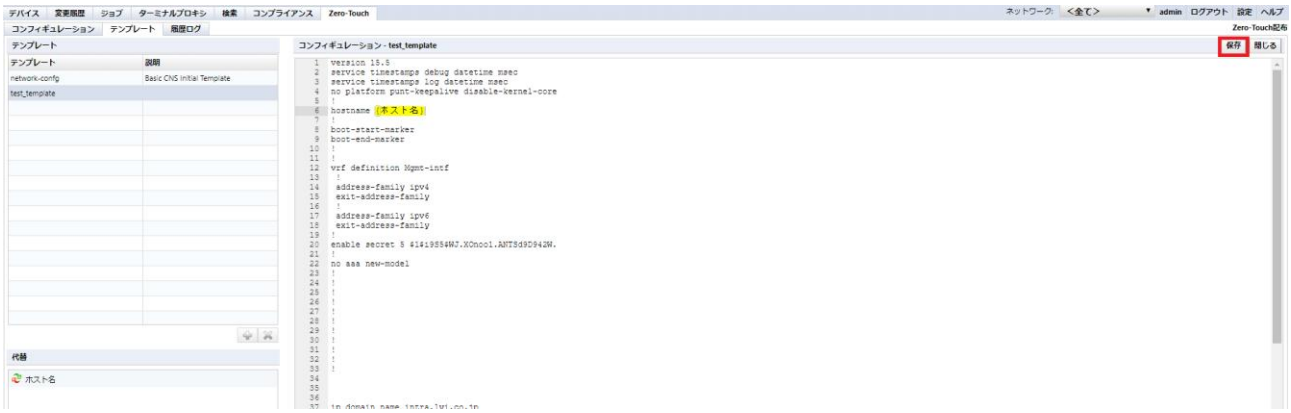
「Compare Against」がデフォルトの {result} に設定されている場合、この正規表現は「Compare Against」の値全体と一致するように設計されません。「Partial Match」を有効にして、正規表現の一部が少なくとも含まれていれば一致としてカウントするように指定しましょう。この設定を行うと、正規表現の一致結果には、一致した uptime が新しい「uptime」列に表示され、後続のノードで {uptime} として使用できます。

また、「Compare Against」を変更することで、これらを連鎖させてより具体的な情報を取得することも可能です。例えば、最近リセットされたスイッチを確認したい場合は、正規表現の一致条件に「day」を含めない稼働時間を確認することができます。「uptime」の正規表現マッチノードを新しい正規表現マッチノードに接続し、正規表現を day に設定します。「Compare Against」を{uptime}に設定し、「Partial Match」を有効にします。

その後、nonMatches の出力を確認するか、このノードを「Email」、「Webhook」、「コンプライアンス違反検出」、または「変数の設定」ノードに接続し、「デバイスが最近リセットされました：{uptime}」といったメッセージを設定することで、別の方法で結果を受け取ることができます。

バルクチェンジで説明したものと同様です。ペーストしたコンフィグに変数を導入し、これをテンプレートにします。

必要な変数をすべて追加したら、テンプレートを保存する必要があります。テキストエリア右上の保存と書かれたボタンをクリックし、作ったテンプレートを保存してください。

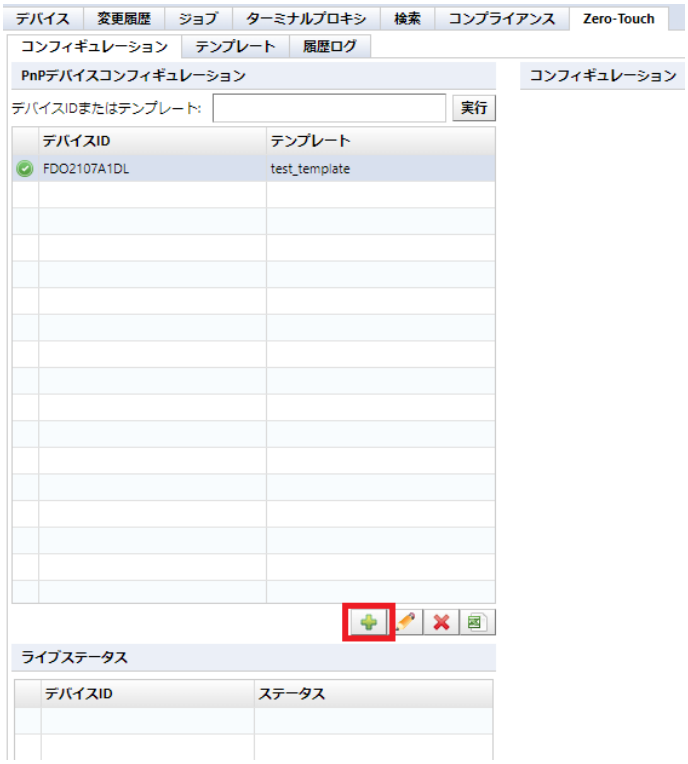


デプロイしたコンフィギュレーションをデバイス内に保存したくない場合は、デプロイするコンフィグの cns config initial...文の最後に、no-persist オプションを追加してください。

(2) デバイスの登録

さて、これで、Zero-Touch に必要なテンプレートの準備が整いました。次に行うことは、設定の配布先となるデバイスの登録です。対象デバイスごとのテンプレート変数の値を設定する必要もあります。

まず、メインペインを*コンフィギュレーション*サブタブに移動してください。そこで、Zero-Touch デバイスコンフィギュレーションの  を押してください。



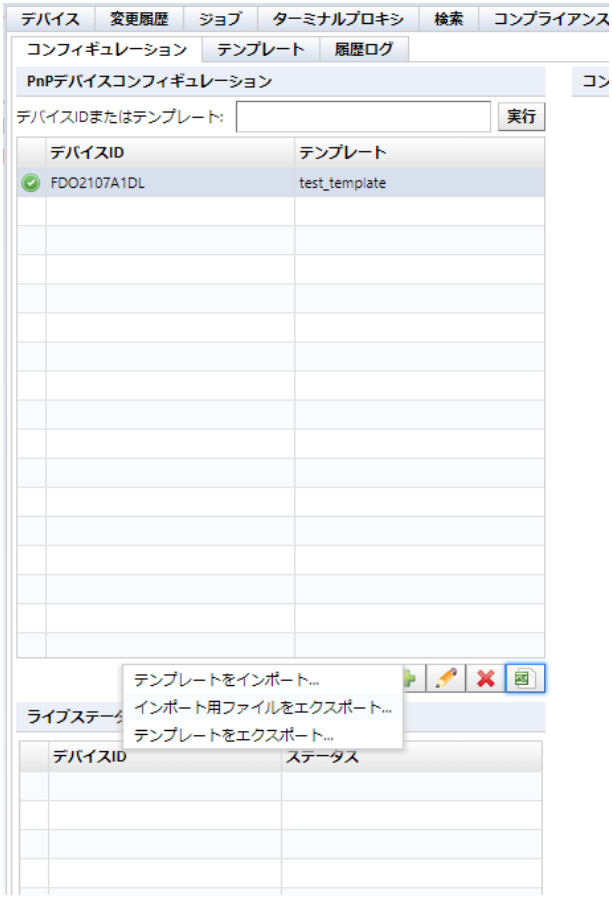
(3) テンプレート変数に入れる値を外部からインポートする

外部にて Excel ファイルで記述されたテーブルを、テンプレートの値として利用することができます。インポートを行うためには、次の手順を追ってください。

Zero-Touch の作業中、デバイスの代替値を入力する所で、閉じるボタンを押してください。

 ボタンを押し、サブメニューを表示してください。

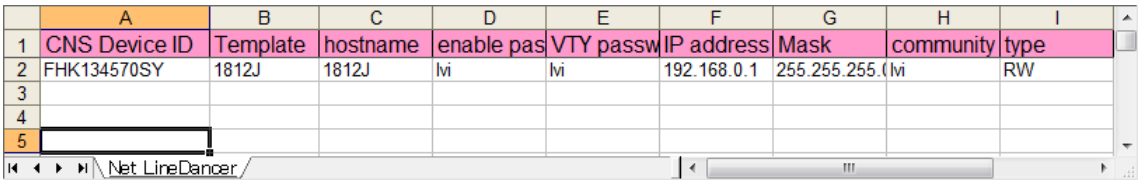
現れたメニューから*インポート用ファイルをエクスポート*あるいはテンプレートをエクスポートメニューから選択してください。



項目	説明
テンプレートをインポート	変数値を格納したエクセルファイルを読み込み、登録します。
インポート用ファイルをエクスポート	値を追記できる空のエクセルシートを出力します。
テンプレートをエクスポート	現在の変数値を反映したエクセルシートを出力します。

7 発展ツール

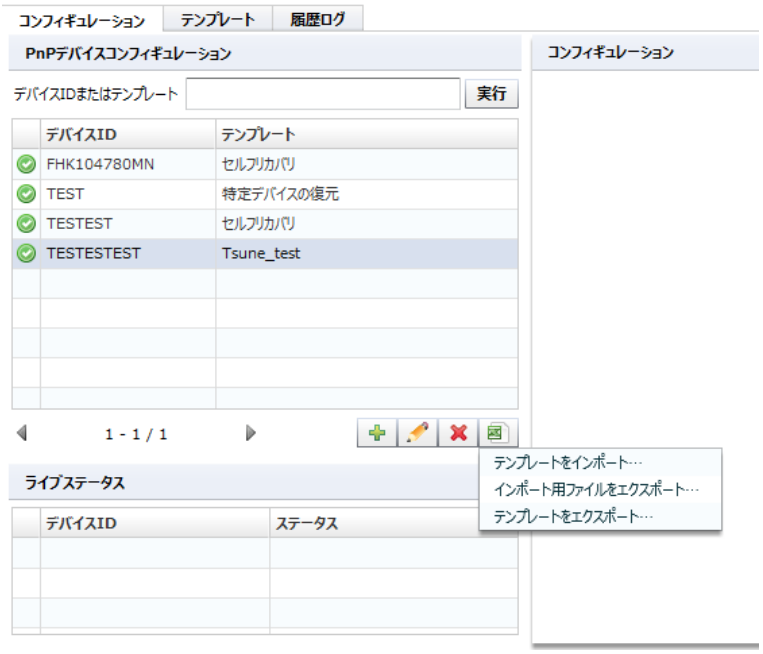
出力されたファイルを編集し、テンプレート変数の値を順番に入力していきます。入力後に保存を行うことを忘れないでください。



	A	B	C	D	E	F	G	H	I
1	CNS Device ID	Template	hostname	enable pas	VTY passw	IP address	Mask	community	type
2	FHK134570SY	1812J	1812J	lvi	lvi	192.168.0.1	255.255.255.(	lvi	RW
3									
4									
5									

Net LineDancer

netLD に戻り、  を再び押し、現れたメニューから *テンプレート*をインポートを押してください。

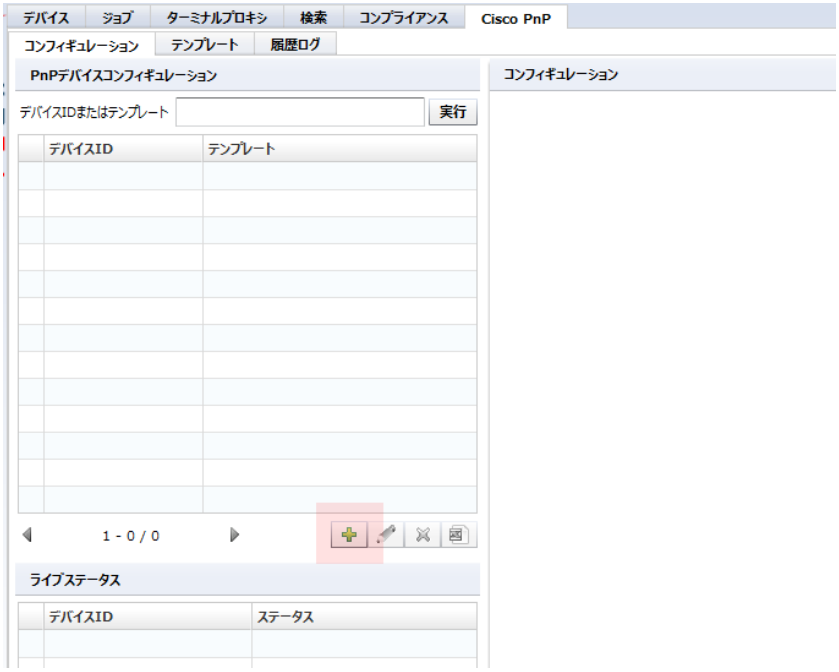


7.2.4.2 セルフリカバリ

Zero-Touch は、新たなコンフィギュレーションを送信する代わりに、それまでに netLD 内部に保存されている他のコンフィギュレーションを送信することができます。この機能は、たとえば現在稼働中のデバイスコンフィグがまちがって消去されてしまった場合に有効です。コンフィグが無くなったデバイスは応答しなくなるため、Zero-Touch のような特殊な機能を用いなくては復旧することができません。

必要な作業はテンプレートをもちいた Zero-Touch と多くの点で共通です。

まず、メインペインでコンフィギュレーションサブタブに移動してください。そして、  を押してください。



デバイスコンフィギュレーションダイアログにて、必要な情報を入力してください。終わったら、OK ボタンを押してください。ただし、配布タイプの項で、セルフリカバリオプションを選択してください。

その後、netLD 内に保存されていたコンフィギュレーションデータがデバイスに書き戻されます。その他にテンプレート配信モードと異なる点はありません。

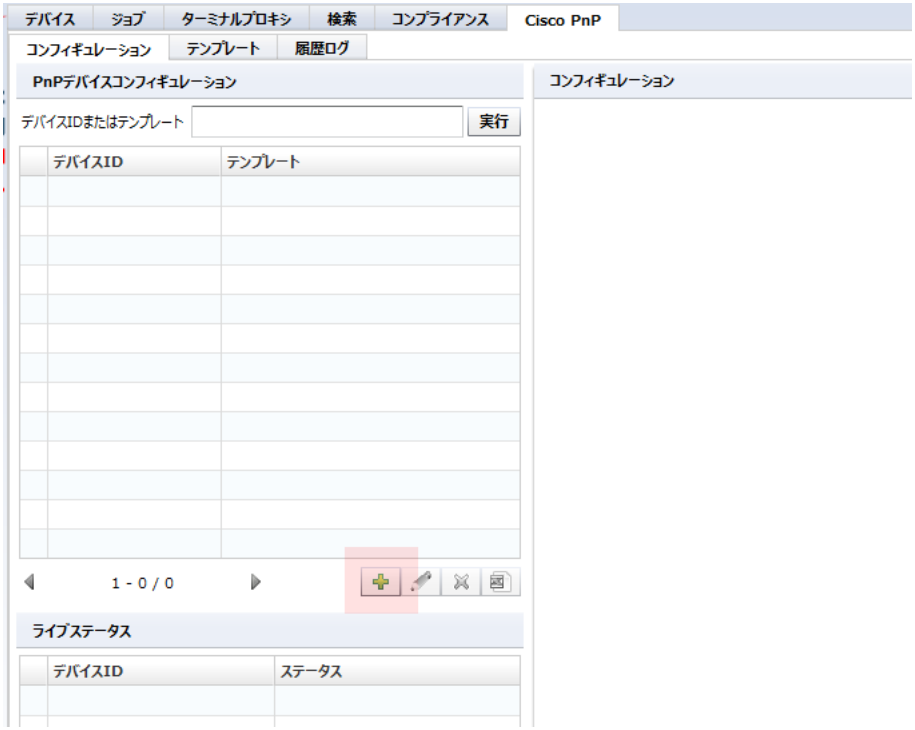
7.2.4.3 特定デバイスの復元

この機能は、古いデバイスを新しいデバイスで入れ替える場合に用います。この機能のおかげで、デバイスが壊れて正常に動かなくなった時でも、新しいデバイスを同じ位置に接続して復旧できます。 このモードで Zero-Touch を実行すると、それまで使っていた古いデバイスのコンフィグが新しいデバイスに書かれます。

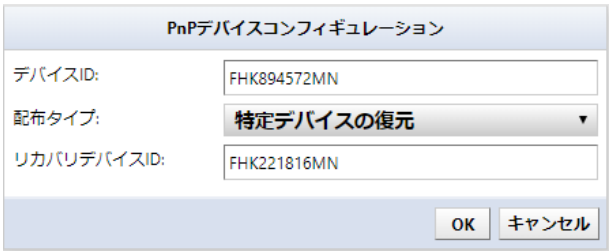
この機能は、デバイスが遠く離れた位置にあって(別のデータセンターなど)、かつ現地に操作を担当できるものがおらず、直接手で操作することができない時に極めて有効です。Zero-Touch を用いれば、現地のデータセンターの人間にケーブルを挿し込むよう電話で指示できればよく、現地の人間に特殊技能は求められません。その後のデバイス復元などの操作が、現地でではなくネットワーク経由で行われるからです。

セルフリカバリと同様、特定デバイスの復元機能は Zero-Touch テンプレート機能とほぼ同様の操作で行うことができます。

まず初めに、メインペインのコンフィギュレーションサブタブを開き、その中に表示されている  を押してください。



Zero-Touch デバイスコンフィギュレーションダイアログ内で、必要な情報を入力します。配布タイプに、*特定デバイスの復元*機能を選択してください。完了後、OK ボタンを押してください。



ここには、リカバリデバイス ID という追加のフィールドがあります。リカバリデバイス ID は一つ目の欄と同じくデバイス ID を指定しますが、この項目には、入れ替え前の古い機器の ID を入力します。

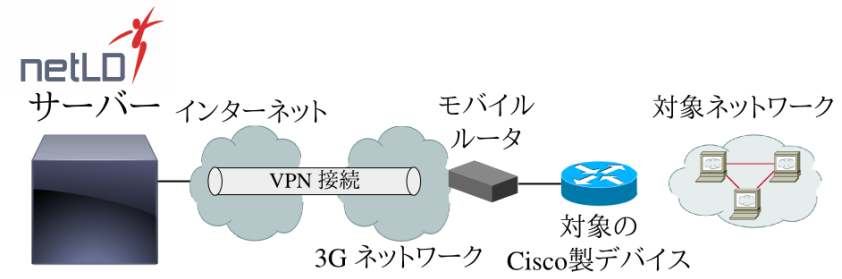
その後、netLD にある、古いデバイス用のコンフィギュレーション情報が、ネットワーク経由で新しいデバイスにアップロードされます。その他の操作方法は Zero-Touch テンプレートの操作方法と同じです。

7.2.5 新規導入デバイスを扱う際の注意

Zero-Touch を用いてコンフィギュレーションをアップロードする際、もしそのデバイスの電源を入れるのが購入してから初めてである場合には、そのデバイスには startup-config が存在しないようにする必要があります。そのようにするためには、ベンダーへのデバイスの発注時に適切な注文オプションを指定してください(例:CCP-CD-NOCF, CCP-EXPRESS-NOCF オプションなど。)

7.2.6 3G ネットワークあるいは VPN 付きモバイルルータ経由での配布

netLD は、コンフィギュレーションを 3G ネットワーク経由で配布することができます。



あるデバイスにコンフィグを配布しないといけないとして、そのデバイスが配置される予定のネットワークで、いくつかのサービスが利用不可である場合を考えてみてください。たとえば、対象のネットワークではインターネットへのアクセスが遮断されているかもしれません。これは、セキュリティを重視しているネットワークでは容易に想像できることです。

遮断は、物理的に接続が無いことが理由のこともあれば、注意深く設定された強力なファイアウォールが稼動しているからかもしれません。デバイスコンフィグの配布のために一時的にファイアウォールを変更するという回答は正しいでしょうか? セキュリティについて厳格であれば、それが極めてリスクを伴うことだという事はお気づきでしょう。

利用不可であるサービスはインターネットに限りません。DNS や DHCP サービスが利用不可なネットワークもありえます。 すべてが静的な IP テーブルで動いているネットワークでは、メンテナンス用のターミナルデバイスを挿入する余地すらないかもしれません。

このような問題が起こるのは、主にその対象ネットワークがあなた自身のものでない時です。たとえば、仮に御社がネットワークのメンテナンス事業を受けおっており、対象ネットワークがあなたの顧客のネットワークである場合です。そのような場合は、3G 接続をうまく活用することができます。なぜなら、3G の無線ネットワークを用いてインターネット

に接続すれば、対象ネットワークを一切利用することなくデバイスと netLD を接続できるからです。

3G を用いる他の大きな利点としては、次のようなものが挙げられます。

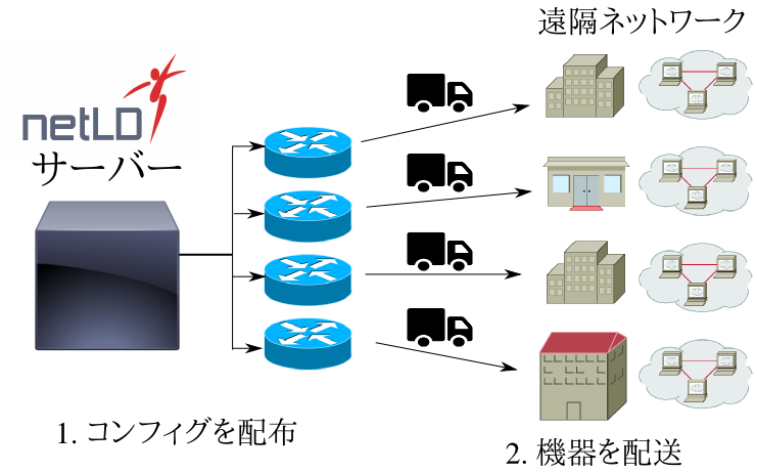
3G 回線からインターネットに接続するためには PPPoE を設定する必要がありません。
3G モバイルルータは再利用できるので、対象ネットワークのあるデータセンターごとに常時準備しておく必要のあるモバイルルータは極少数です。そのため、必要経費は限定的です。

以下の説明では、3G ベースのコンフィグ配布方法について簡単に説明します。

Zero-Touch タブにて、Cisco デバイスにコンフィグを配布するのに必要な設定をあらかじめすべて行なっておきます。つまり、テンプレートを作り、デバイス ID を登録することが含まれます。
モバイルルータの電源を入れ、データセンターへの VPN 接続を有効にします。
新たな Cisco 製デバイスを モバイルルータに接続します。
netLD がデバイスからのリクエストを自動的に受け取り、コンフィギュレーションを 3G ネットワーク経由で送信します。
配布が終了したあと、電話などで対象ネットワークの近くにいる管理要員に指示し、デバイスにネットワークケーブルを差し込みます。そうすれば、デバイスはデータセンターのネットワークに正しく接続されます。

7.2.7 デバイスを手元で設定してから遠隔地に送付する場合

デバイスを遠隔地に送付するもうひとつの方法は、デバイスを手元で設定してから遠隔地に宅配便で送付する方法です。



ただ単純に、Zero-Touch を用いて手元でデバイスにコンフィグを書き込み、その後デバイスを遠隔地に送付します。この手法の良い点は極めてシンプルでわかりやすいことですが、悪い点は、デバイスを一旦手元に取り寄せるための手間と経費がかかってしまうことです。デバイスを製造元から直接遠隔地に送る必要がある場合には、この手法を使うことはできません。

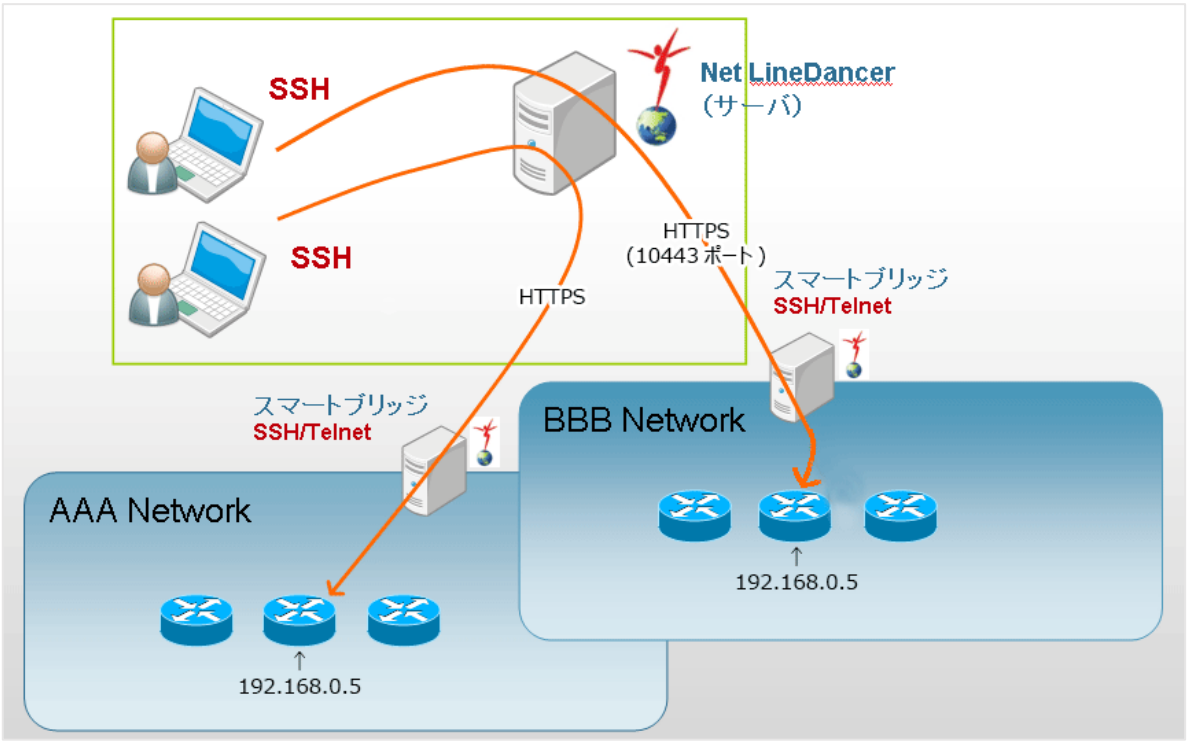
7.2.8　ブートストラップコードの配布

DHCP の利用が不可能なネットワークでのコンフィギュレーション配布には、ブートストラップコードを予め送付しておくという追加の操作が必要になります。下に示すものは、Zero-Touch のためのブートストラップ例です。<IP>の部分を、実際の netLD サーバの IP アドレスに読み替えてください。

```
cns id hardware-serial
!
cns connect cns-profile ping-interval 10 retries 3 sleep 5
discover interface FastEthernet
template cns-profile
!
cns template connect cns-profile
cli description Basic CNS Initial Template
cli ip address dhcp
cli ip route 0.0.0.0 0.0.0.0 ${interface}
cli no shutdown
exit
!
cns config initial <IP> status http://<IP>/cns/config.asp
!
end
```

7.3　スマートブリッジ（オプション）

スマートブリッジとは、MSP サービス事業におけるマルチテナントをサポートするためのオプションです。例えば、異なるネットワーク内で同じ IP アドレスが存在する場合でも、それぞれのネットワークにスマートブリッジを設置することで、IP アドレスを個別に識別し、管理できます。

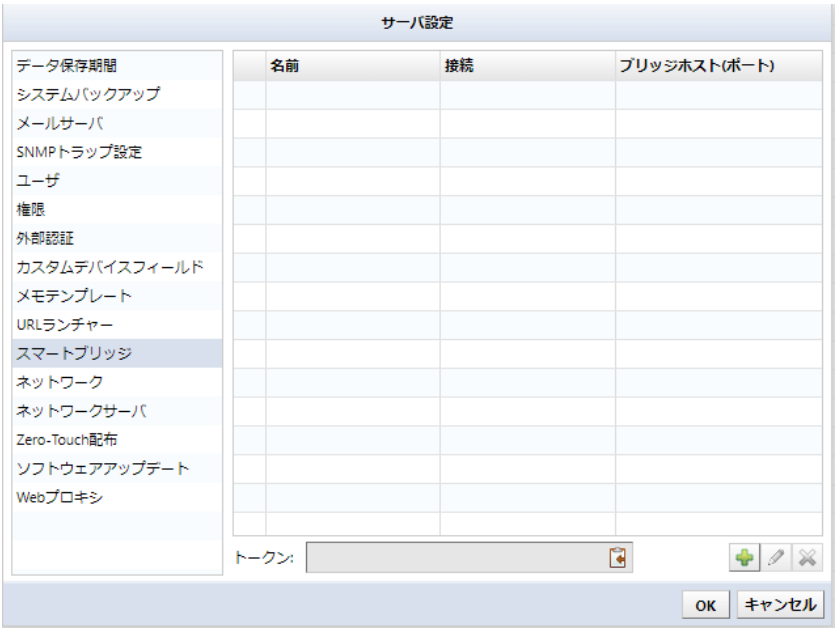


スマートブリッジを使用すると、負荷分散の利点もあります。スマートブリッジは、前回のバックアップからの差分データのみをコアサーバに送信するため、各 netLD サーバの CPU 使用率や回線使用量の削減が期待できます。

7.3.1 コアサーバへの登録

スマートブリッジを netLD サーバに登録する必要があります。

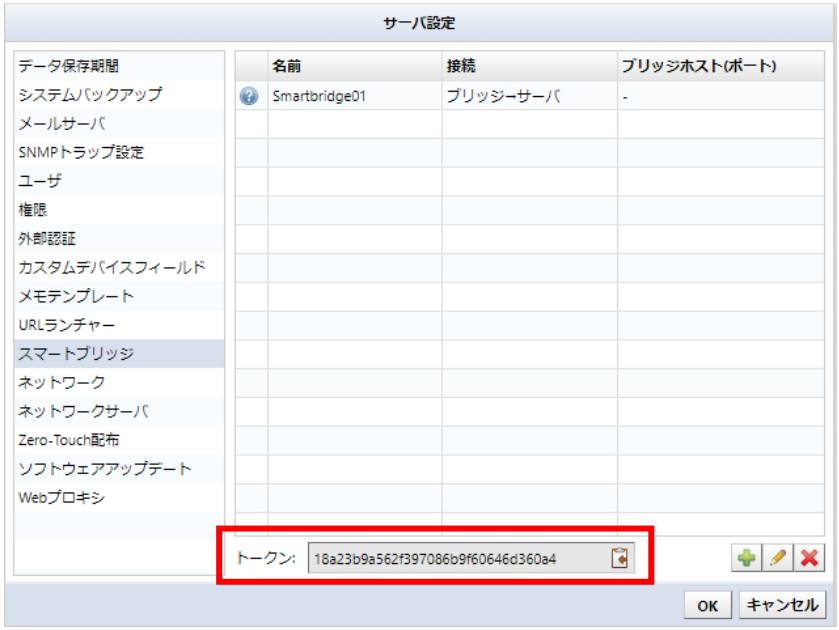
サーバ設定ウィンドウ→スマートブリッジを開き、  ボタンをクリックします。



スマートブリッジの情報を入力します。

項目	説明
名前	スマートブリッジの名前を入力します。
接続	接続方向を次の中から選択します。 「ブリッジ→サーバ」、「サーバ→ブリッジ」
ホストまたは IP	スマートブリッジのホスト名または IP アドレスを指定します。 ※接続に「サーバ→ブリッジ」を選択した場合に表示されます。
ポート	スマートブリッジの待ち受けポートを指定します。 ※接続に「サーバ→ブリッジ」を選択した場合に表示されます。

スマートブリッジをコアサーバに追加すると、新しく追加されたスマートブリッジが一覧に表示されます。各スマートブリッジには、認証用の固有の「トークン」があります。トークンは、インストール後にスマートブリッジをコアサーバに接続するときに指定する必要があります。一覧からスマートブリッジを選択し、サーバ設定ウィンドウの下部からトークンをコピーすることができます。



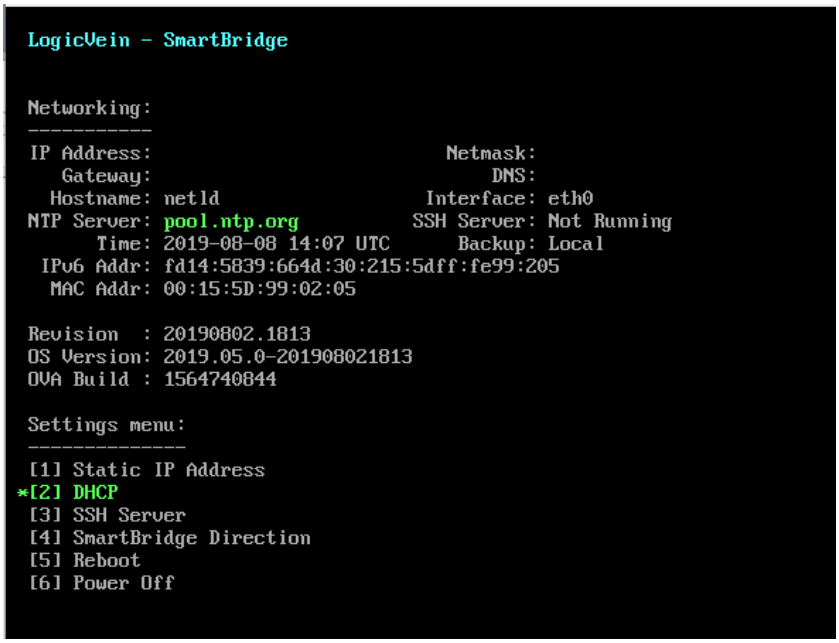
一覧の左端のアイコンは、接続状態を表します。上図の  は、まだ接続が確立されていないことを示しています。正しく接続されると、アイコンが  に変わります。

正しく接続できない場合は、再度設定を行ってください。問題が解決しない場合は、カスタマーサポートにお問い合わせください。

7.3.2 ネットワーク設定

スマートブリッジのインストール方法は、netLD コアサーバのインストール方法と同様です。詳しくは、2.1 インストールするを参照してください。

デプロイが完了したら、マシンをパワーオンしてネットワーク設定を行います。デフォルトでは、IP アドレスなどは DHCP から取得されます。DHCP サーバがない環境では、下図のように、IP アドレスなどが未設定になります。

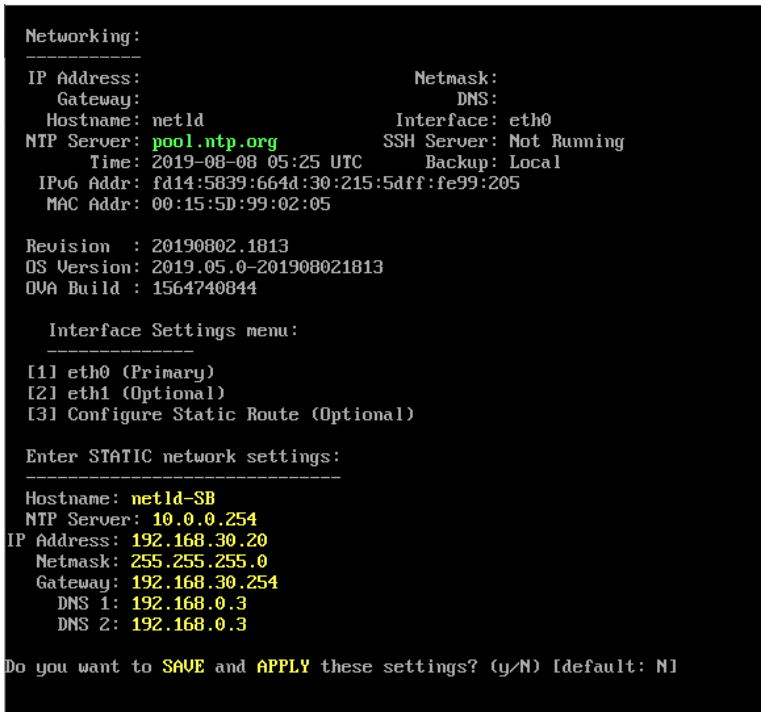


手動で IP アドレスを設定する場合は、以下の手順で設定します。設定はキーボードを使って行います。

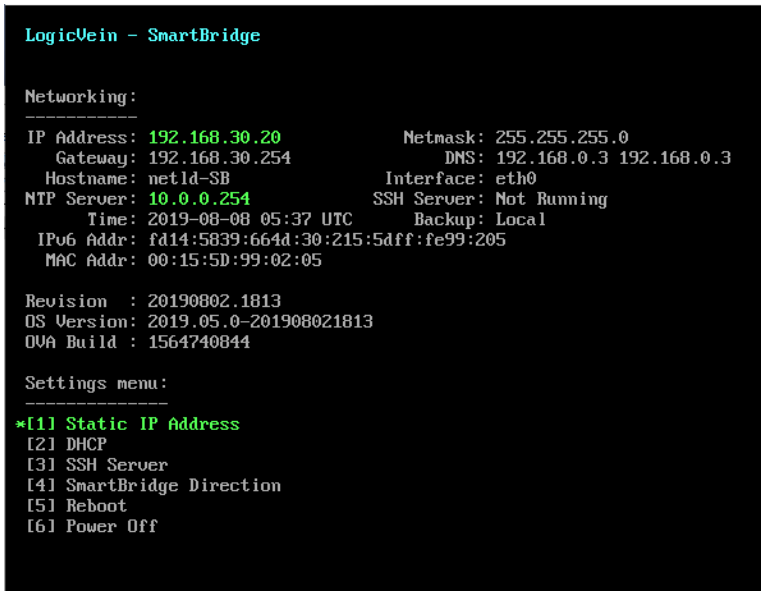
1. キーボードの「1」を押し、［Static IP Address］を選択します。
2. キーボードの「1」を押し、［eth0 (Primary)］を選択します。
3. 以下のネットワーク設定項目が順に表示されます。キーボードで値を入力し、「Enter」キーを押して次へ進みます。

パラメータ	説明
Hostname	使用するホスト名を入力
NTP Server	NTP サーバの IP アドレスを入力
IP Address	使用する IP アドレスを入力
Netmask	サブネットマスクを入力
Gateway	デフォルトゲートウェイの IP アドレスを入力
DNS 1/2	DNS サーバの IP アドレスを入力（必須ではありません。）

4. 「y」を押して設定を保存します。



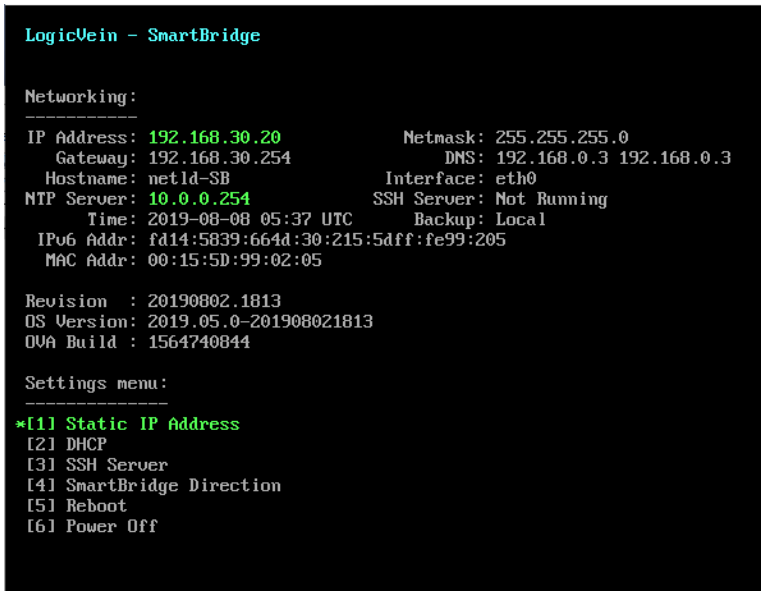
以上でネットワーク設定は完了です。



7.3.3 接続方向の設定

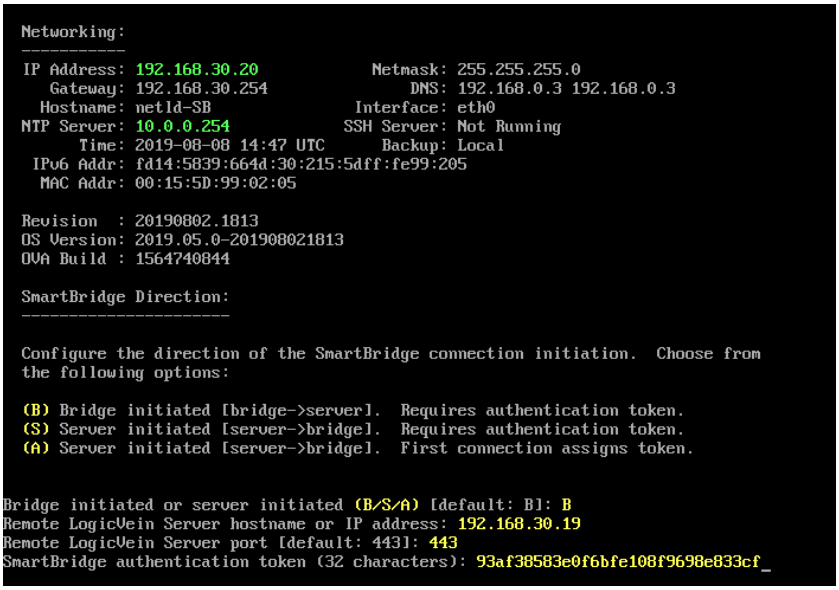
スマートブリッジの接続の方向を設定するには、次の手順を実行します。設定はキーボードを使って行います。

1. キーボードの「4」を押し、［SmartBridge Direction］を選択します。



2. 以下の項目の値をキーボードで入力し、「Enter」キーを押して次へ進みます。

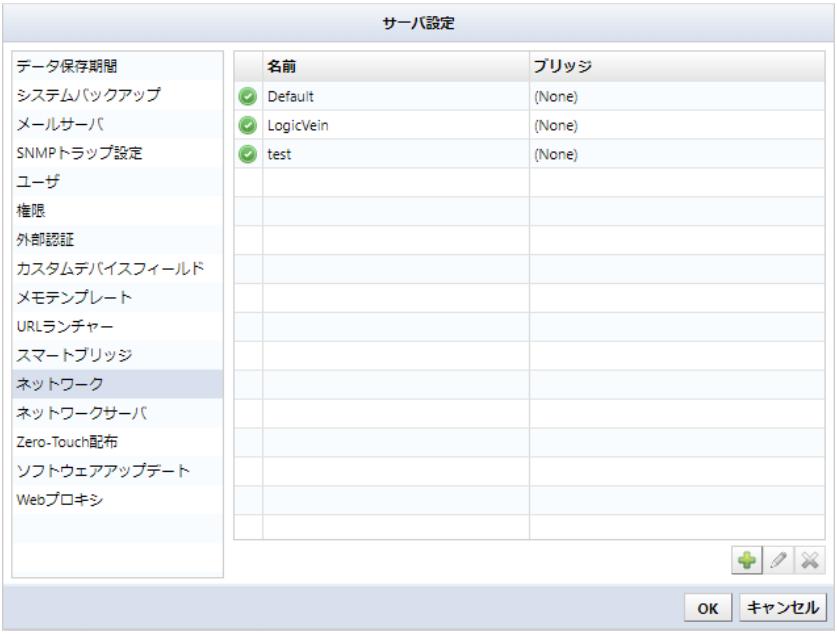
パラメータ	説明	入力例
Initiation	接続方向（B/S/A） B：ブリッジからコアサーバに接続する（トークンあり） S：コアサーバからブリッジに接続する（トークンあり） A：コアサーバからブリッジに接続する（トークンなし）	B
Hostname or IP address	netLD コアサーバの IP アドレス ※接続方向に「B」（サーバ→ブリッジ）を選択した場合に表示されます。	192.168.0.1
Port	待ち受けポート（デフォルト：443）	443
Token	32 文字のトークンを入力します。 トークンを取得するには、「2107.3.1 コアサーバへの登録」を参照してください。 ※接続方向に「B」「S」（トークンあり）を選択した場合に表示されます。	7ccb5……



設定が完了すると、画面は最初の設定画面に切り替わります。

7.3.4　スマートブリッジで管理するネットワークの作成

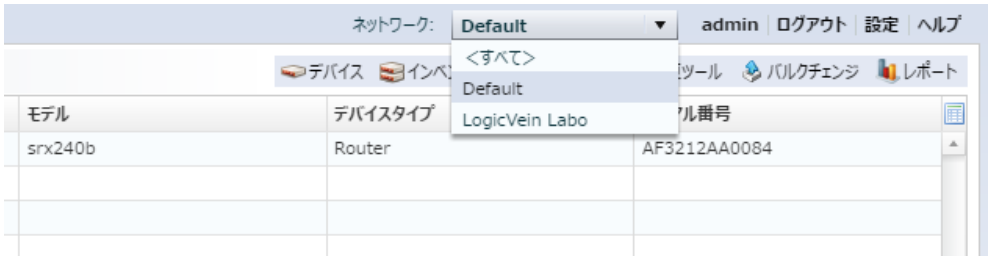
スマートブリッジごとに、管理するネットワークを作成する必要があります。サーバ設定ウィンドウ→ネットワークを開きます。



ボタンをクリックし、表示されたダイアログで各項目を設定します。ブリッジホストから登録されているスマートブリッジを選択します。最後に、OK ボタンを押してください。

項目	説明
名前	管理ネットワークの名前
ブリッジホスト	使用するスマートブリッジを指定します。登録されているスマートブリッジが選択肢として表示されます。
ジャンプホストを使用する	ジャンプホストを使用する場合にチェックを入れます。 ジャンプホストの詳細については「7.4 ジャンプホスト」を参照してください。

以上の操作でネットワークが追加されます。ネットワークが追加されると、画面右上に「ネットワーク」という項目が表示され、管理ネットワークを切り替えることができます。



※ 追加したネットワークごとに、クレデンシャルやプロトコルなどを設定する必要があります。詳しくは、「5.2 クレデンシャル」、「5.4 プロトコル」を参照してください。

7.3.5 スマートブリッジの運用

スマートブリッジが管理するネットワークにデバイスを追加します。デバイスの追加方法については、「6.3 デバイスの追加」を参照してください。以降、スマートブリッジが管理するネットワークでは、スマートブリッジが netLD サーバに代わって情報収集などを行います。

7.4　ジャンプホスト

ジャンプホストはあるネットワークへデバイスログインする場合に決められた PC やデバイスからでないとアクセス出来ない環境がある場合に威力を発揮します。

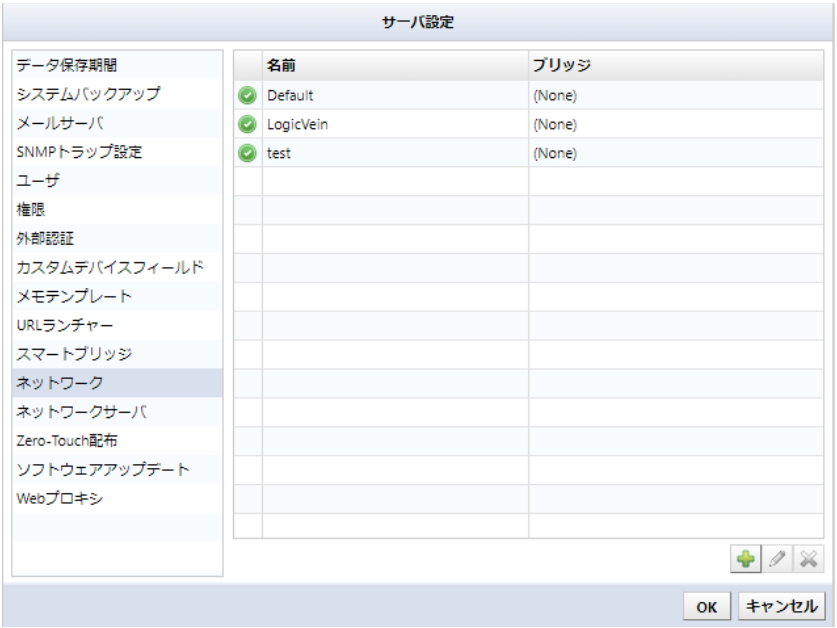
ジャンプホストを設定すると netLD は中間のデバイスにログインし、そのデバイスからコンフィグバックアップを行いたいデバイスに対してコマンド発行をします。

この機能はスマートブリッジと同じような機能ですが、以下の点が異なります。

	ジャンプホスト	スマートブリッジ
インストール	不要	必要
OS	Linux or Cisco IOS	Virtual Appliance
機能	制限あり	コアサーバと同じ
対応プロトコル	ジャンプホスト	コアサーバと同じ

ジャンプホストを使用したネットワークの作成

ジャンプホストを使用するには、スマートブリッジと同様にネットワークを作成します。設定→ネットワークの順に開いてください。



ボタンをクリックし、ダイアログ内の必要な情報を入力してください。ジャンプホストを使用するにチェックを入

れ、ジャンプホストの IP アドレス、ログインに必要なユーザ名/パスワードを入力します。最後に、OK ボタンを押してください。

項目	説明
名前	ネットワークの名前（任意）
ブリッジホスト	スマートブリッジを使用する場合にプルダウンメニューから選択します。 詳細は「スマートブリッジ」を参照してください。
ジャンプホストを使用する	チェックを入れます。
IP アドレス	ジャンプホストの IP アドレスを入力します。
ユーザ名	ジャンプホストにログインする為のユーザ名を入力します。
パスワード	入力したユーザのパスワードを入力します。
アダプタ	使用するアダプタを入力します。 Redhat Linux か Cisco IOS をプルダウンメニューから選択します。

以上でネットワークが追加されました。スマートブリッジと同様にネットワークが追加されると、グローバルメニューに「ネットワーク」という項目が追加され、ネットワークを切り替えることが可能です。

7.5　外部 NMS との連携

この章では、外部 NMS ソフトウェアと連携させる際の手順について解説します。

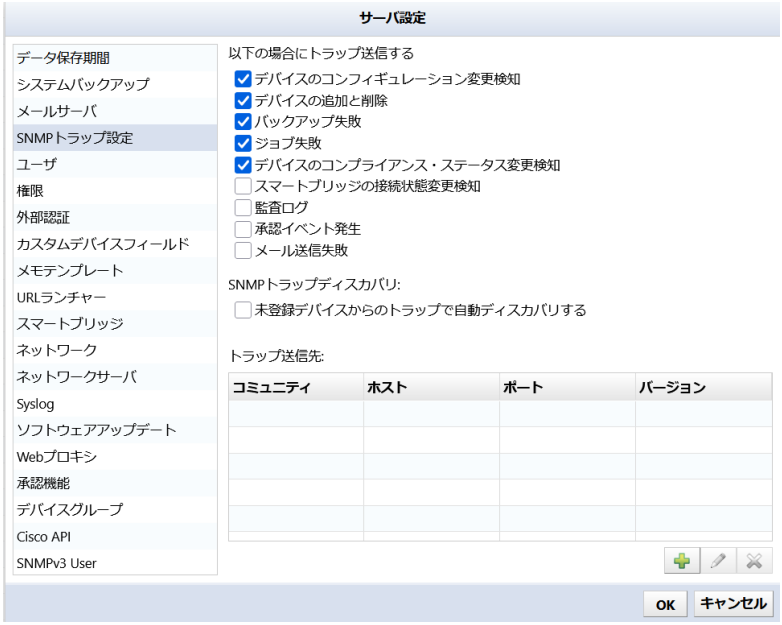
SNMP トラップを設定する

netLD は、以下のいずれかの条件が満たされた時に、他の NMS ネットワーク管理ツールに対してトラップを発信します。

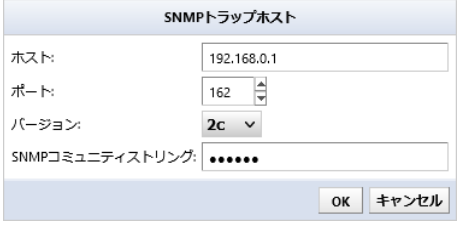
- デバイス コンフィギュレーションが変更された場合
- 新たなデバイスが netLD インベントリに追加、あるいはそこから削除された場合
- netLD バックアップジョブが失敗した場合
- いずれかのデバイスにてコンプライアンス状態が変化した場合
- ジョブが失敗した場合
- スマートブリッジ使用時に、接続状態が変化した場合
- netLD にログイン/ログアウト/ログイン失敗した場合
- ジョブの承認イベントが発生した場合
- メールの送信に失敗した場合

トラップの送信先を編集するためには、以下の手順を踏んでください。

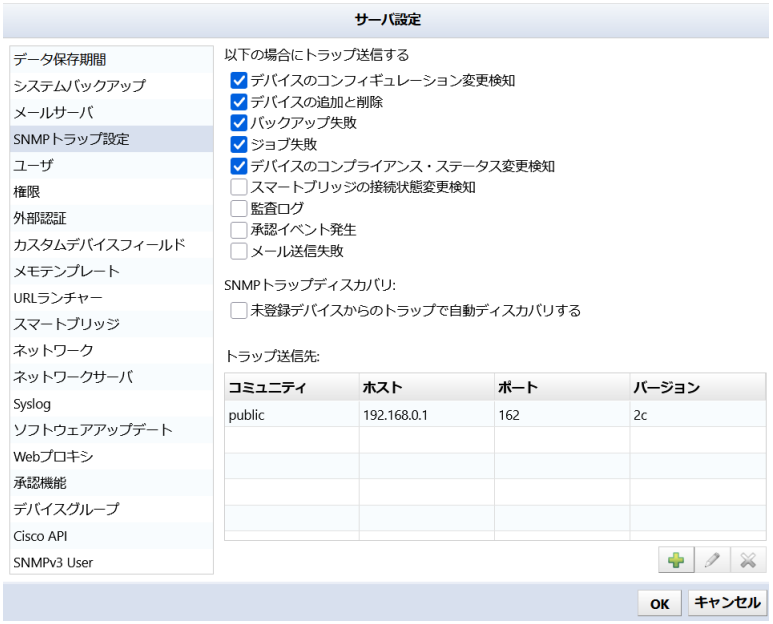
設定→SNMP トラップ設定から、どの条件で netLD がトラップを送信するかのオン、オフを選択してください。



トラップ送信先リストの下にある  ボタンを押し、送信先のホスト名、ポートを設定してください。SNMP コミュニティストリングの欄には、トラップコミュニティ名を入力してください。OK ボタンを押してください。



指定した送信先が正しくリストに追加されていることを確認し、OK ボタンを押して変更を保存、ウィンドウを閉じてください。



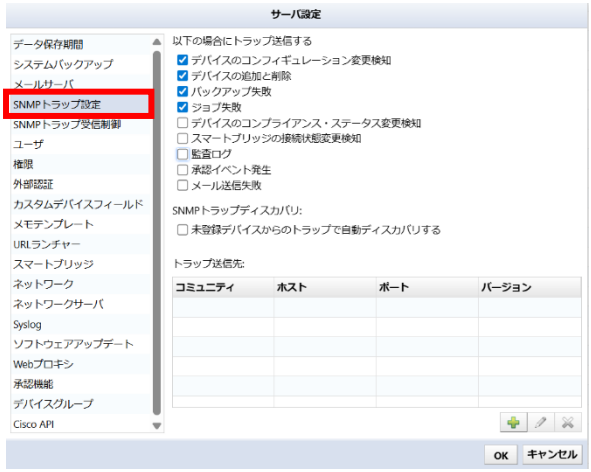
7.5.1 SNMP トラップディスカバリ

r20251003.0827 より SNMP トラップディスカバリの機能に対応しました。この機能をオンにする事で、netLD に登録されていないデバイスから SNMP トラップを受信した場合、その送信元 IP アドレスに対して自動的にディスカバリを実行します。製品に複数のネットワークが設定されている場合、サーバはトラップの送信元 IP アドレスをもとにヒューリスティック手法を用いて、そのデバイスが属するネットワークを判定します。

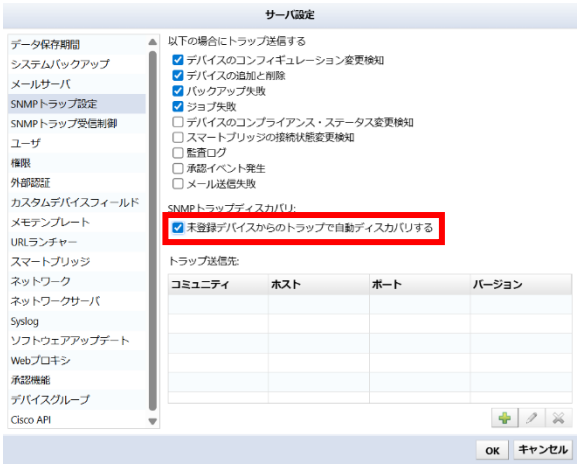
補足	*ヒューリスティック手法*とは、サブネットマスクの一致度や既知の管理 IP 情報などの推定ルールに基づき、送信元 IP アドレスから最も適合度の高いネットワークを自動的に判断する方式です。

ディスカバリを成功させるには、あらかじめ該当ネットワークの SNMP クレデンシャル情報を設定しておく必要があります。また、過剰なディスカバリの試行を防ぎ、同一ネットワーク内の複数デバイスからのトラップをまとめて処理できるようにするため、ディスカバリの実行までに最大数分の遅延が発生する場合があります。ディスカバリに失敗したデバイスからの後続トラップは、5 分間は無視され、その後再びディスカバリが試行されます。一度ディスカバリされ登録された後に削除されたデバイスは、サーバが再起動されるまで再びディスカバリの対象にはなりません。また、デバイスを削除した後は SNMP トラップディスカバリを行ってもデバイス登録は行われません。

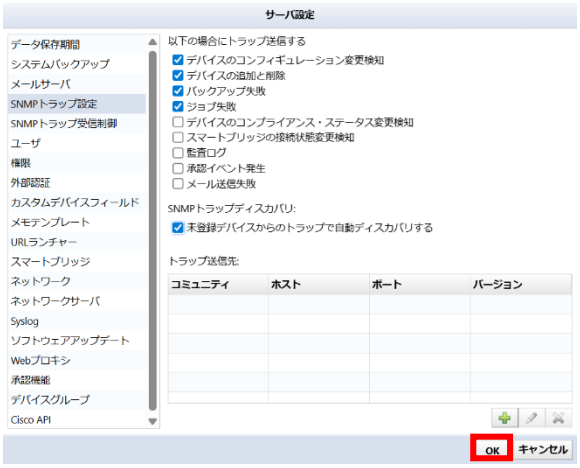
1. グローバルメニューの［設定］をクリックし、［SNMP トラップ設定］を選択します。



2. 未登録デバイスからのトラップで自動ディスカバリするにチェックをいれます。



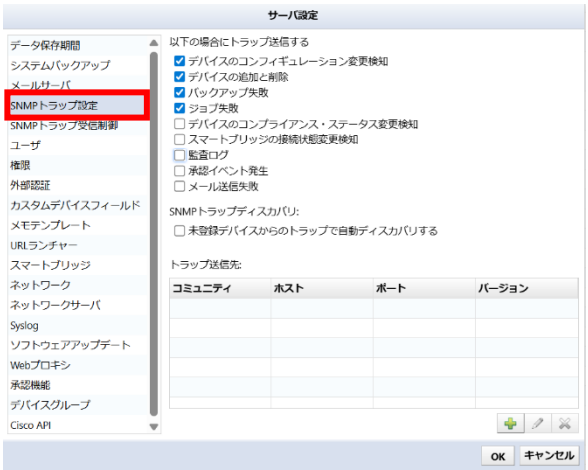
3. 設定を有効にする為に、サーバ設定の下にある[OK]をクリックします。



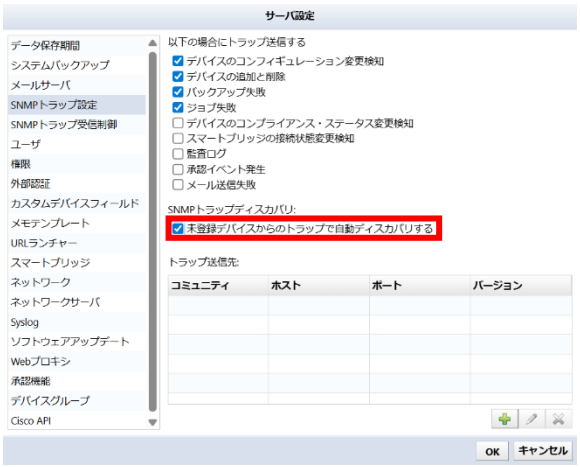
7.5.1.1 SNMPv1/v2 でトラップを受信する

SNMP v1/v2 トラップで送信されるコミュニティ文字列を検証し、有効なもののみを受け付けるようにする場合は、[SNMP トラップユーザ]であらかじめ許可するコミュニティ文字列を指定する必要があります。これらが定義されている場合、一致するコミュニティ文字列を持つトラップのみが受信され、それ以外は拒否されます。この機能を使用する為には、あらかじめ SNMP トラップ設定で SNMP トラップディスカバリの機能を有効にしておく必要があります。

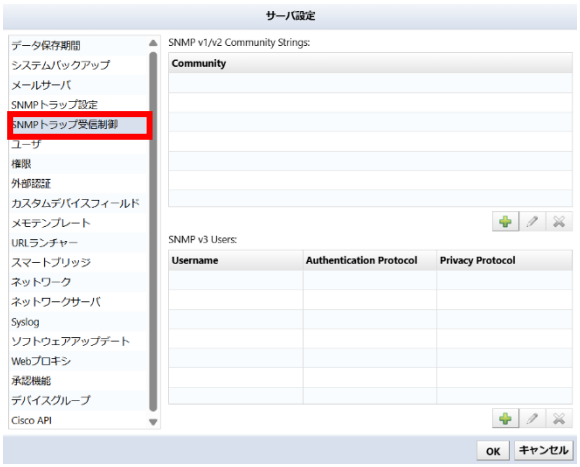
1. グローバルメニューの［設定］をクリックし、［SNMP トラップ設定］を選択します。



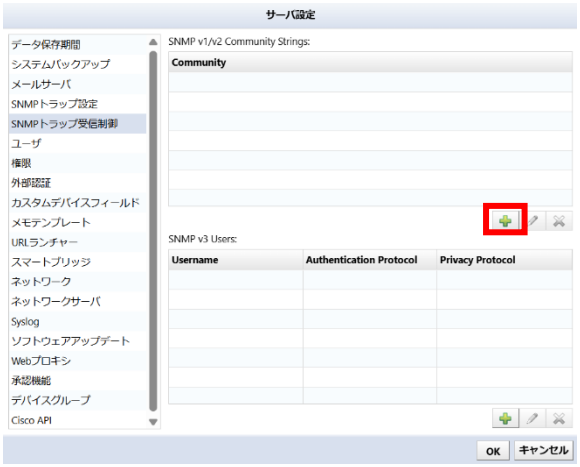
2. 未登録デバイスからのトラップで自動ディスカバリするにチェックをいれます。



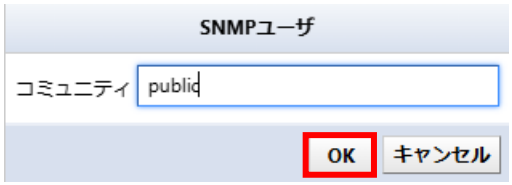
3. ［SNMP トラップ受信制御］を選択します。



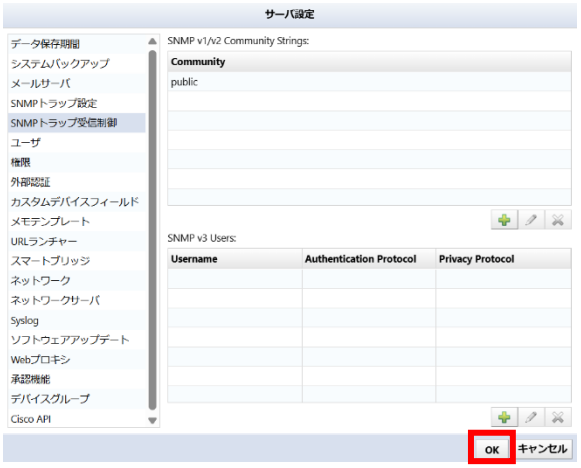
4. SNMPv1/v2 テーブルの下にある[ ]をクリックします。



5. 受信する SNMP トラップの認証に使用されるコミュニティ文字列を入力します。
6. [OK]をクリックします。



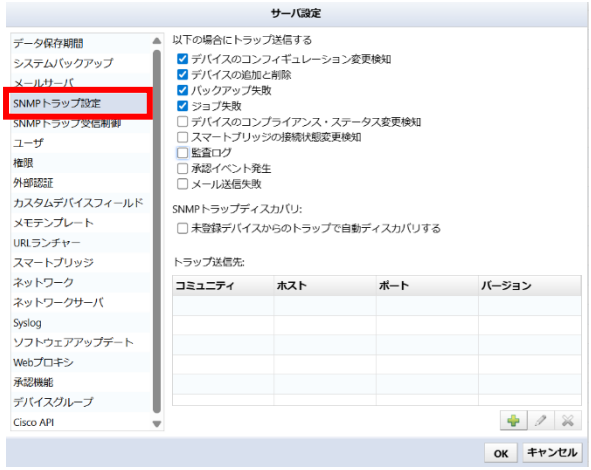
7. 設定を有効にする為に、サーバ設定の下にある[OK]をクリックします。



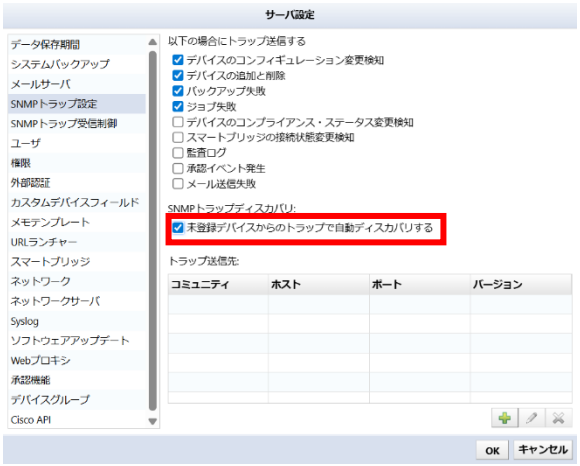
7.5.1.2 SNMPv3 でトラップを受信する

SNMPv3 トラップを有効なもののみを受け付けるようにする場合には、netLD が受信した SNMP トラップを認証または復号化できるように事前に認証情報を設定する必要があります。この機能を使用する為に、あらかじめ SNMP トラップ設定で SNMP トラップディスカバリの機能を有効にしておく必要があります。

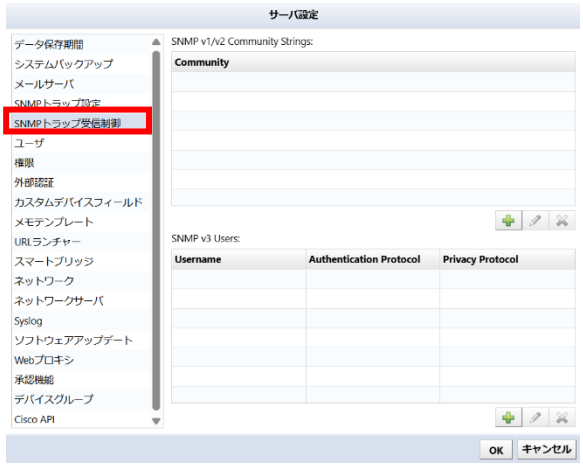
1. グローバルメニューの［設定］をクリックし、［SNMP トラップ設定］を選択します。



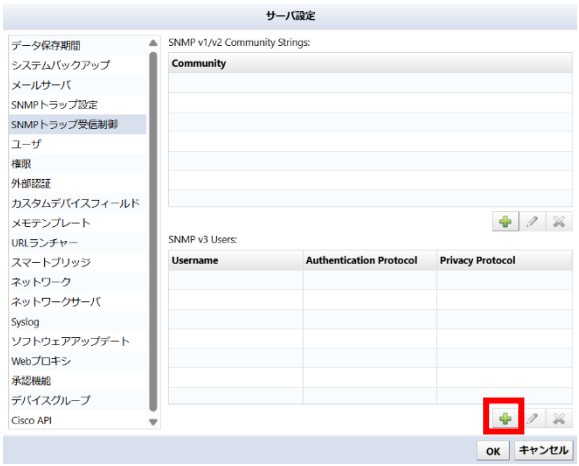
2. 未登録デバイスからのトラップで自動ディスカバリするにチェックをいれます。



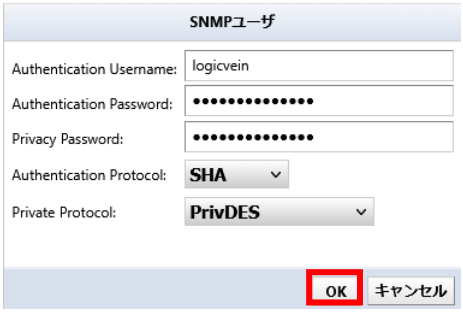
3. ［SNMP トラップ受信制御］を選択します。



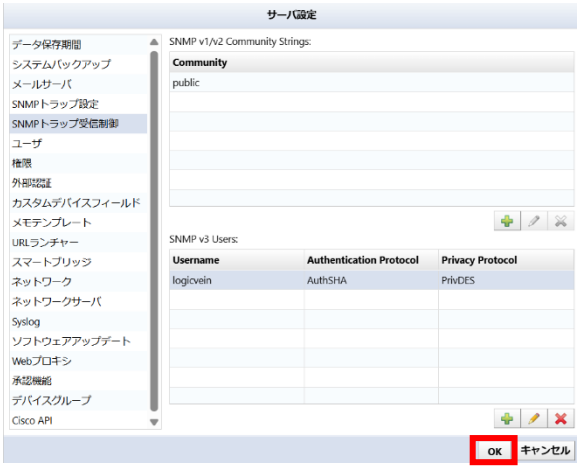
4. SNMPv3 テーブルの下にある[ ]をクリックします。



5. SNMPv3 ユーザ情報を設定します。これは、受信する SNMP トラップの認証または復号化に使用されます。
6. [OK]をクリックします。



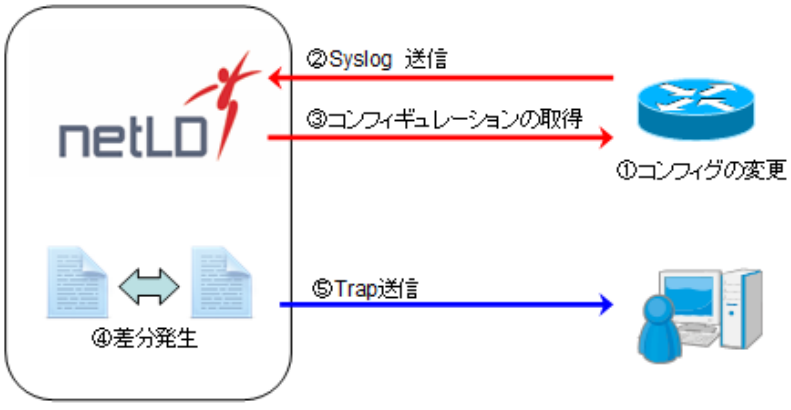
7. 設定を有効にする為に、サーバ設定の下にある[OK]をクリックします。



7.6 リアルタイムバックアップ

netLD は、netLD を仲介しない外部からのコンフィギュレーション変更に対しても、リアルタイムで変更検知及びバックアップを行うことができます。変更検知は Syslog メッセージを利用して行います。

この機能はデバイスそれぞれの機能を使用するにあたり 3 つの留意点があります。



まず、全てのデバイスがこの機能に対応しているわけではないことにご注意ください。検知のためには、必要とされる情報を syslog にロギングできる必要があります。ここで、必要な情報をロギングできないデバイスは、リアルタイム変更検知のサポート対象外となります。また、Syslog の設定方法はデバイス、ベンダーによって様々ですので、その設定

方法の解説については、デバイス製造元によるマニュアルを参照するか、製造元のサポートをご利用ください。

最後に、お客様のネットワークが、デバイスから netLD サーバへロギングすることができない環境である場合、お客様のローカルネットワーク内に外部 Syslog サーバを設置する必要があります。外部 Syslog サーバの使用については、別途お問い合わせください。

7.6.1 デバイスの設定

この機能を有効にするためには、Syslog メッセージを netLD に送信するよう、各デバイスを設定する必要があります。 Syslog のロギングを有効にするコマンドはベンダーやモデルにより異なるため詳細はここでは省略致しますが、いくつか Syslog ロギングの設定例をご紹介します。

以下の 2 つは、それぞれ Cisco 製品 およびヤマハ製品に対する設定例です。この例では、netLD サーバの IP アドレスを 192.168.0.10 としています。

Cisco 2600

```
Router# configure terminal
Router(config)# logging 192.168.0.10
Router(config)# logging on
Router(config)# exit
```

Yamaha RT107

```
Yamaha# syslog host 192.168.0.10
Yamaha# syslog info on
Yamaha# save
```

7.6.2 動作チェック

リアルタイム変更検知の動作確認を行うには、netLD サーバのリアルタイムイベントログを確認します。netLD のログファイルは、netLD.log というファイル名で netLD のインストール先フォルダに保存されます。リアルタイム変更を検知した時、つぎの例のようなメッセージ netLD.log ファイルに書きこまれます。

```
[RealtimeProvider] [Jetty-1] INFO - Added device 10.0.0.152 to real-time batch.
```

netLD.log ファイルに上記のようなエントリが見つからない場合、また別の Syslog ログファイルを確認し、対象デバイスからメッセージを受信していることを確認してください。netLD のビルトイン Syslog サーバを使用している場合、Syslog は syslog.log というファイル名で netLD のインストール先フォルダにあります。現在の netLD リアルタイム変更検知は、機器ベンダーやモデルの全てをサポートしているわけではありません。

7.7　デバイスの EOS/EOL 管理

EOS/EOL を管理するために、インベントリに「製品終了（EOS)」/「サポート終了（EOL)」のカラムが追加されました。EOS/EOL 情報は、手動または Excel ファイルからのインポートで設定が可能であるほか、Cisco デバイスのみ Cisco Support API を利用して自動設定が可能です。

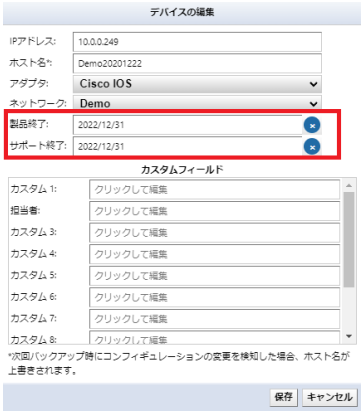
7.7.1　手動で設定

7.7.1.1　手順

1. EOS/EOL を取得する機器を選択します。

2. デバイスメニューから「デバイスプロパティの編集」をクリックします。

3. 製品終了とサポート終了の日付を選択し保存をクリックします。



以上の手順により、カラムに設定した日付が表示されるようになります。

7.7.2 自動で設定

7.7.2.1 前提条件

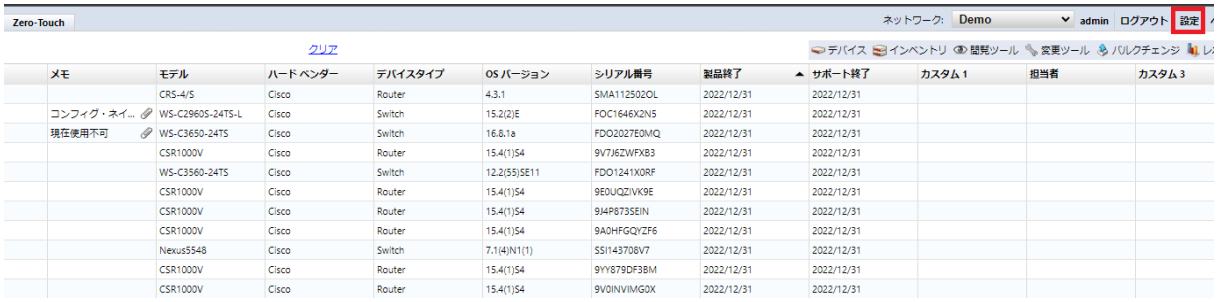
- 使用しているサーバがインターネットに接続できること
- Cisco Smart Net Total Care にアクセスするための、事前に Cisco アカウントでログインし、API キーとシークレットコードを取得する必要がある

※ 有効な Cisco Smart Net Total Care (SNTC)が必要です。

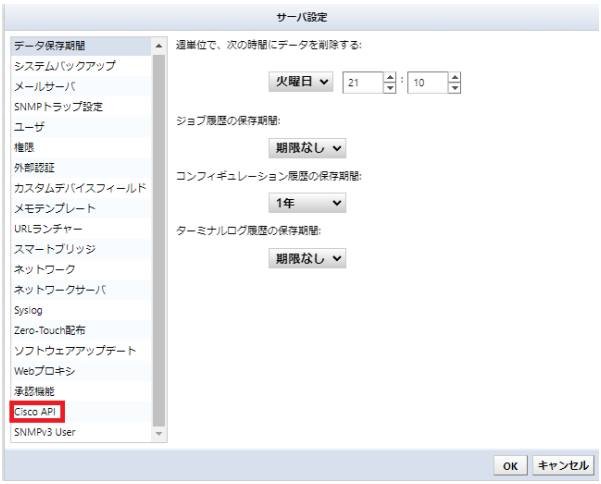
※ API の取得について、以下を参照してください。
(https://developer.cisco.com/docs/support-apis/#!user-onboarding-process)

7.7.2.2 手順

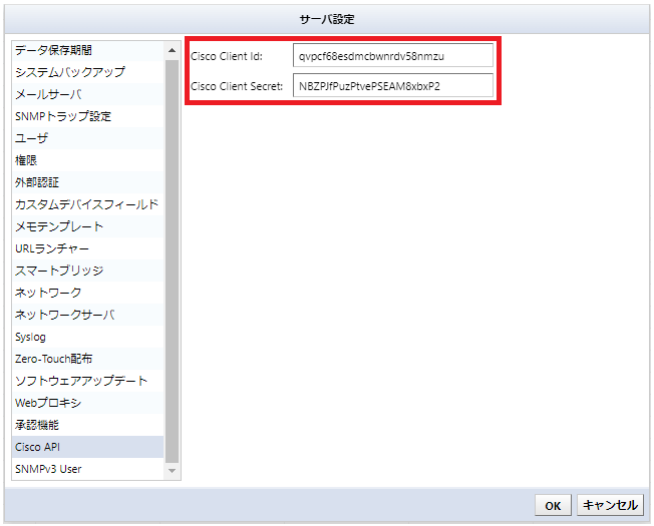
1. 設定をクリックします。



2. CiscoAPI をクリックします。



3. API キーとシークレットコードを入力し、OK をクリックします。

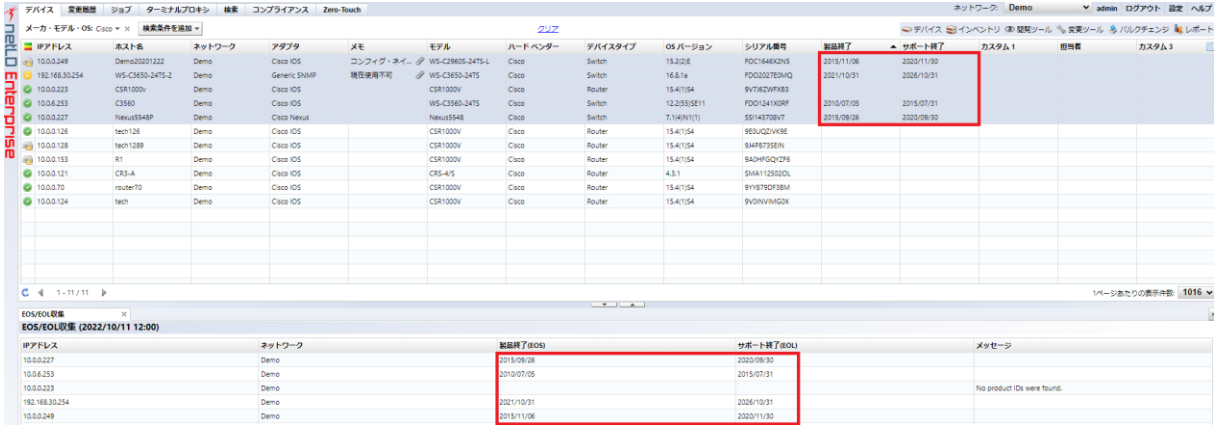


4. EOS/EOL を取得する機器を選択します。

5. デバイスメニューから「Cisco デバイスの EOS/EOL 情報の収集」をクリックします。

6. 以下の画面で「はい」をクリックします。

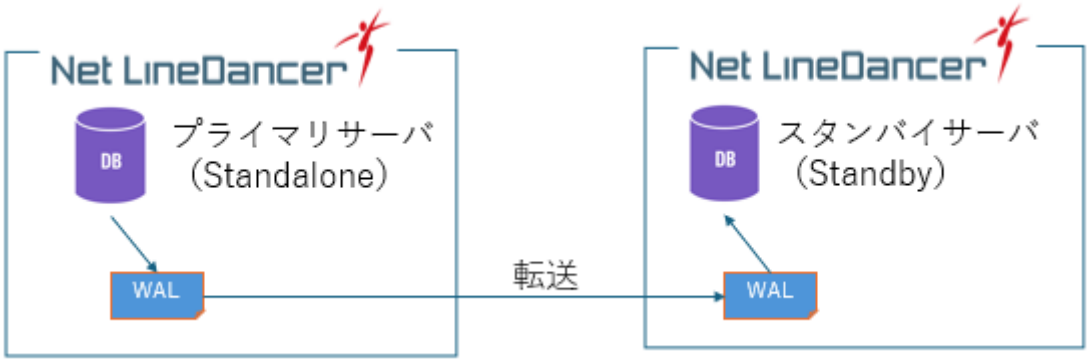
以上の手順により、自動で EOS/EOL 情報を取得し、カラムに登録します。



8. 冗長機能

8.1 概要

リビジョン 20241218.0941 より、冗長機能がサポートされました。冗長機能では、「Standalone」と「Standby」という 2 つの役割を使用します。Standalone では、通常どおり監視や設定を行います。Standby は、Standalone からのトランザクションログ（以後、WAL）を受信し、それをリカバリすることで同期を行います。



※ Standalone は冗長構成において「プライマリサーバ」と呼ばれます。

※ OS イメージやデバイスの詳細の添付にアップロードされたファイルについては、120 秒間隔でスタンバイサーバに同期されます。

8.1.1 利用条件

冗長機能は、eth1 を使用してデータを同期します。SSH を使用するため、プライマリサーバとスタンバイサーバ間にファイアウォールがある場合は、スタンバイサーバからプライマリサーバへの SSH 通信を許可してください。また、両サーバの CPU コア数、メモリ容量、ディスクサイズは同一である必要があります。

8.1.2 制限される機能

冗長機能には以下の制限があります。これらの機能はサポートされていませんので、ご注意ください。

- スマートブリッジとの同時使用
- AWS や Azure などのクラウド環境での使用
- プライマリサーバで受信した Syslog データの引き継ぎ
- プライマリサーバで取得したシステムバックアップファイルの引き継ぎ
- OVA コンソールで設定する内容の引き継ぎ

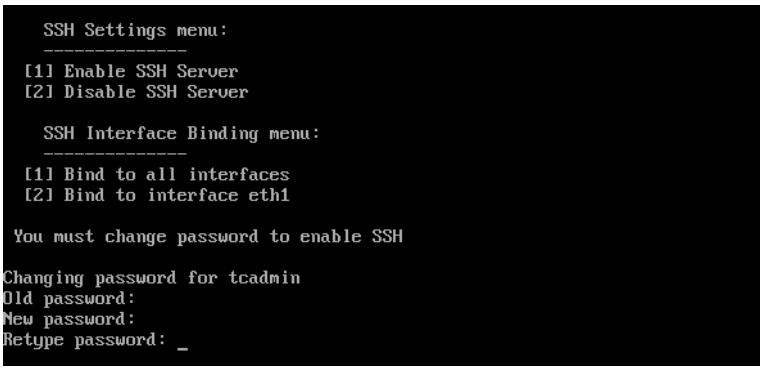
8.2 設定

冗長構成の設定は、OVA コンソールを使用して行います。この設定を実施するためには、VMware や Windows Hyper-V を操作できる権限を持つユーザが必要です。

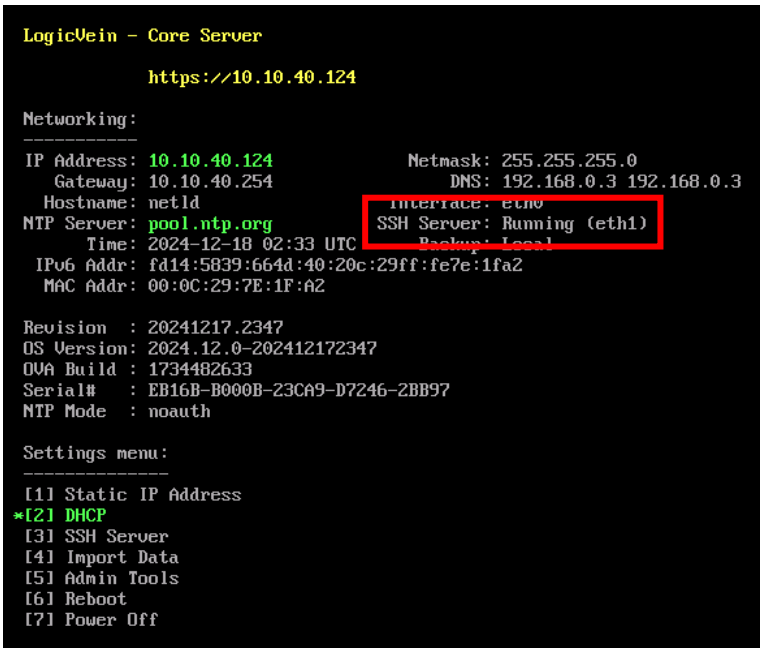
8.2.1 手順

設定を行う前に、プライマリサーバとスタンバイサーバの eth1 インタフェースに IP アドレスを設定し、eth1 間で通信可能な状態にしておいてください。

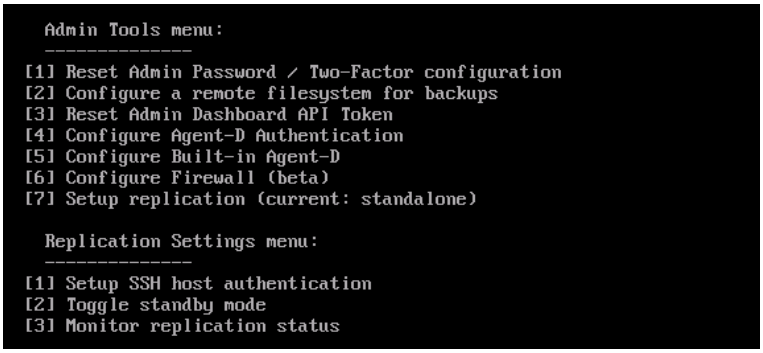
1. プライマリサーバの OVA コンソールに接続します。
2. キーボードの[3](SSH Server)->[1](Enable SSH Server)->[2](Bind to interface eth1)と押下し、eth1 に対して SSH を有効にします。



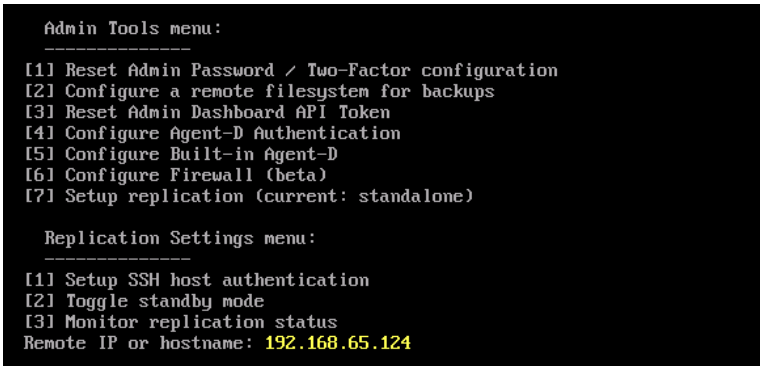
3. SSH Server が Running になっていることを確認します。



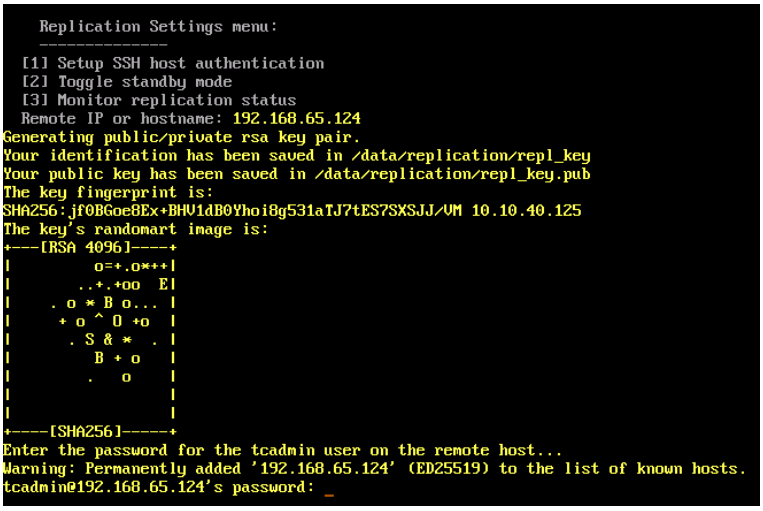
4. スタンバイサーバの OVA コンソールに接続します。
5. キーボードの[5](Admin Tools)->[7](Setup replication)->[1](Setup SSH host authentication)と押下し、プライマリサーバの SSH ホスト認証設定をします。



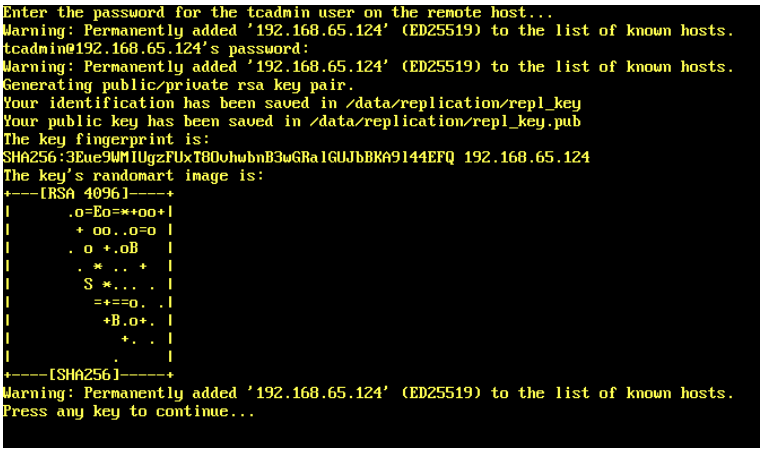
6. プライマリサーバの eth1 の IP アドレスを入力します。



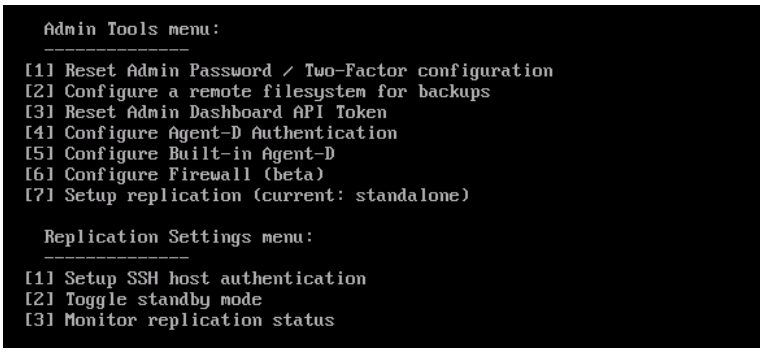
7. プライマリサーバへ SSH する時のパスワードを入力します。



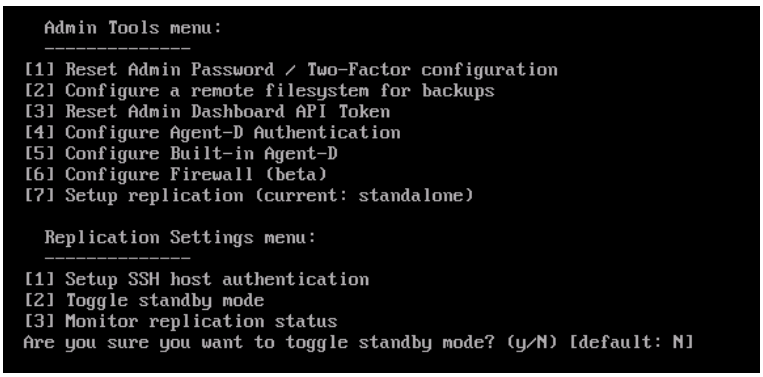
8. Enter キーなど何かキーを押下します。



9. キーボードの[5](Admin Tools)->[7](Setup replication)->[2](Toggle standby mode)と押下し、スタンバイサーバをサーバの役割を Standalone から Standby に変更します。



10. 「y」を押下します。

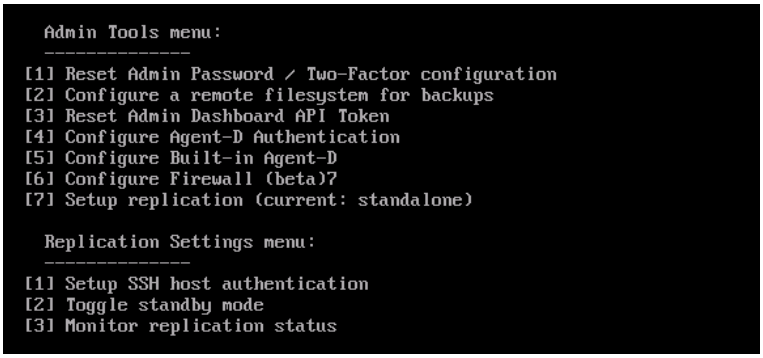


設定は以上です。「y」を押下すると、自動でスタンバイサーバが再起動されます。

8.2.2　ステータスの確認

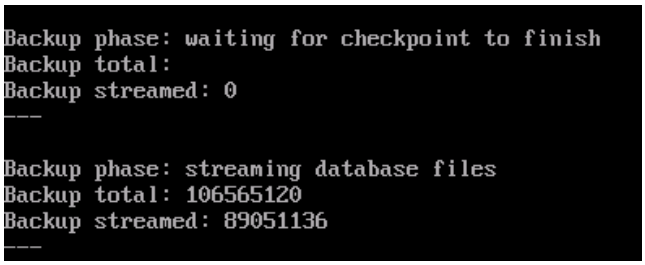
冗長機能のステータスは、OVA コンソールから確認することができます。

1. プライマリサーバの OVA コンソールに接続します。
2. キーボードの[5](Admin Tools)->[7](Setup replication)->[3](Monitor replication status)と押下し、ステータスを確認します。



※ステータスが表示されると自動で更新されていきます。ステータス画面を閉じるには、ctrl+c を押してください。

冗長構成が設定されると、まずはバックアップフェーズが開始されます。バックアップフェーズでは、初期データがプライマリサーバからスタンバイサーバにコピーされます。



バックアップフェーズが完了すると、データストリーミングが開始されます。開始されると、以下のような画面が表示されます。設定後は、”Replication state: streaming”が表示されることを確認します。

8.2.3　再設定が必要ケース

以下のケースでは、再度冗長機能の設定が必要です。

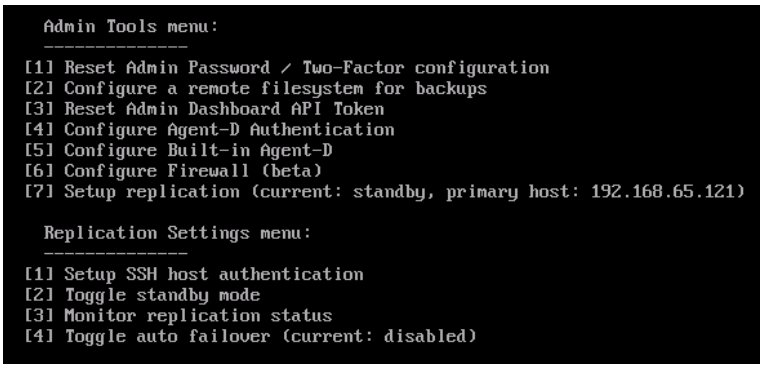
- プライマリサーバでシステムバックアップを復元した場合
- フェイルオーバー後、元の状態に戻す場合

8.3 フェイルオーバー

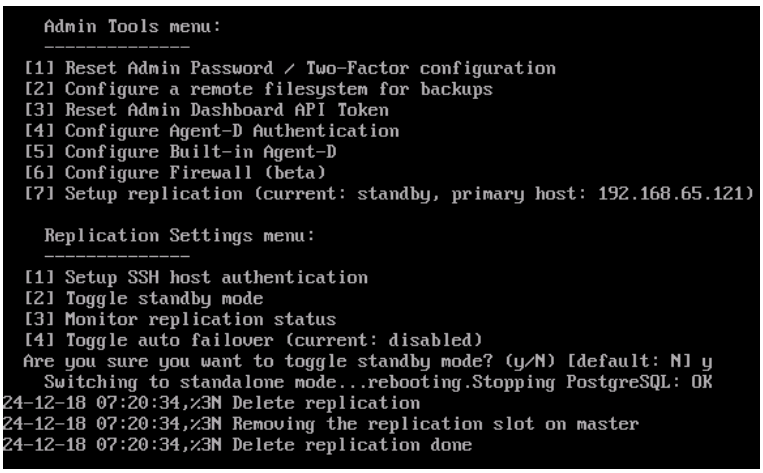
8.3.1 手動フェイルオーバー

スタンバイサーバで監視を行う場合には、役割を Standby から Standalone に変更します。変更手順は以下のとおりです。

1. スタンバイサーバの OVA コンソールに接続します。
2. キーボードの[5](Admin Tools)->[7](Setup replication)->[2](Toggle standby mode)と押下し、スタンバイサーバをサーバの役割を Standby から Standalone に変更します。



3. 「y」を押下します。



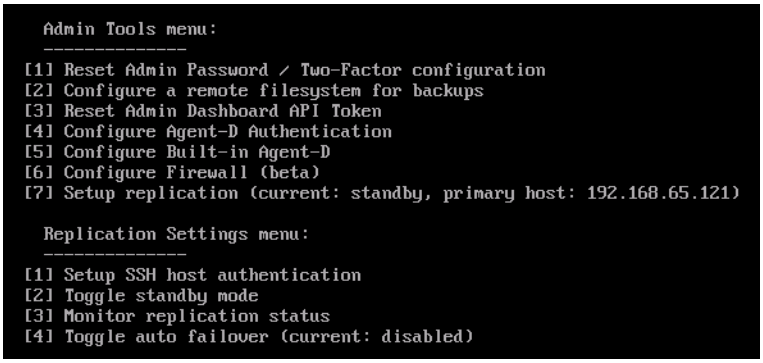
「y」を押下すると、自動でスタンバイサーバが再起動されます。再起動後、Web ブラウザからログインしてください。

8.3.2 自動フェイルオーバー

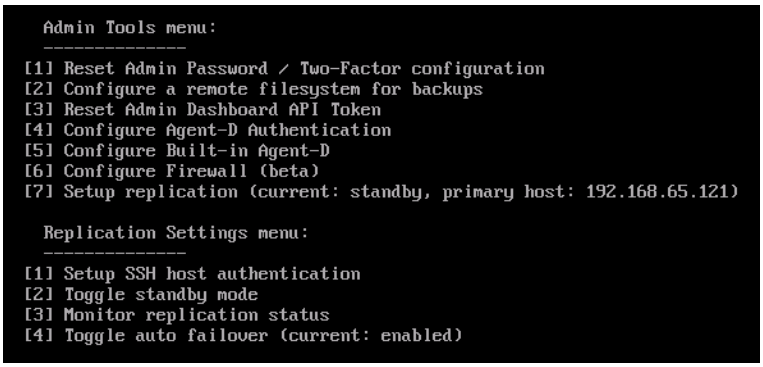
自動フェイルオーバーを有効に設定すると、プライマリサーバとスタンバイサーバ間で 60 秒以上の意図しない通信断が発生した場合、スタンバイサーバが自動で役割を Standby から Standalone に変更し、監視を引き継ぎます。ユーザがプライマリサーバを再起動/シャットダウンした場合、または 60 秒以内の再接続に成功した場合、切り替わりは行われません。

デフォルトでは、自動フェイルオーバーは無効に設定されています。プライマリサーバに障害が発生した場合に、スタンバイサーバが自動的に監視を引き継ぐようにするには、次の手順に従って自動フェイルオーバーを有効に設定します。

1. スタンバイサーバの OVA コンソールに接続します。
2. キーボードの[5](Admin Tools)->[7](Setup replication)->[4](Toggle auto failover)と押下し、自動フェイルオーバーを有効にします。



3. [4]を押下後、自動で最初の画面に戻ります。再度、[5](Admin Tools)->[7](Setup replication)と進み、Toggle auto failover の current が「enabled」になっていることを確認します。



9. その他ツール

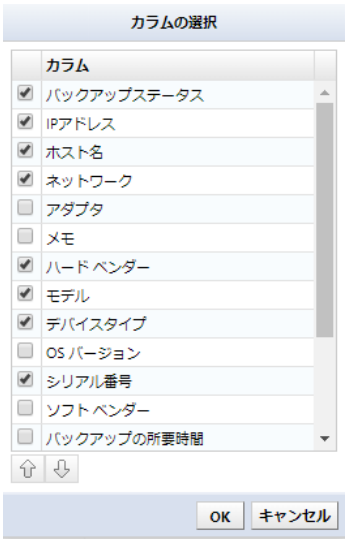
この章では、netLD の使い勝手やセキュリティを向上させるための様々な tips を解説します。また、そこまで使われる頻度の少ないものの、時と場合によって重要になるようなツールについても解説します。

9.1 デバイスビューの表示列を変更する

デバイスビューの表示列を変更するには、右上の  ボタンを押してください。カスタムダイアログが現れるので、表示したい要素のチェックボックスをオンにしてください。

右上の  ボタンを押してください。

チェックボックスを設定します。



9.2　スケジュールフィルタ

ジョブスケジュールをフィルタするために、cron 表現を用いることができます。ここで追加したフィルタは、後にジョブを計画する際に再利用することができます。

ジョブ→ジョブ管理→フィルタの設定を開きます。

ボタンを押し、フィルタを作ります。

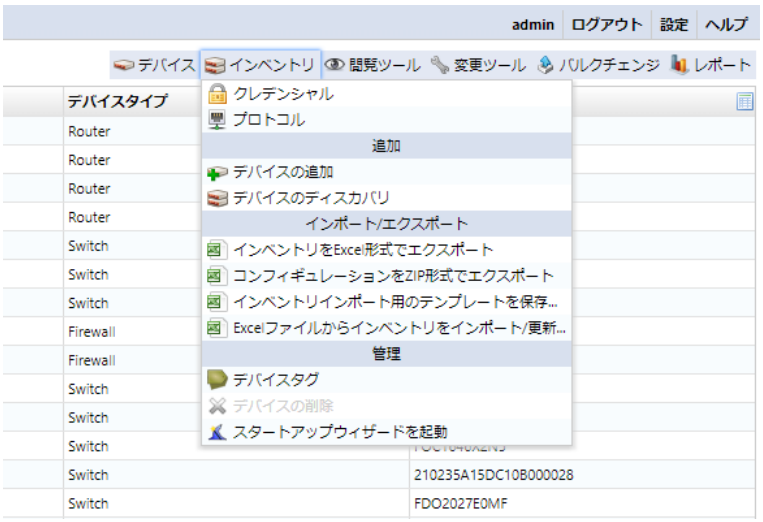
名前と cron 表現を、対応する欄に入力します。OK ボタンを押してください。

新しいフィルタが追加されているのを確認できたら、OK ボタンを押して終了します。

9.3　デバイスタグ

netLD インベントリ内のデバイスは、タグによって管理することができます。デバイスタグは検索中に利用することができます。

インベントリ→デバイスタグを選択します。

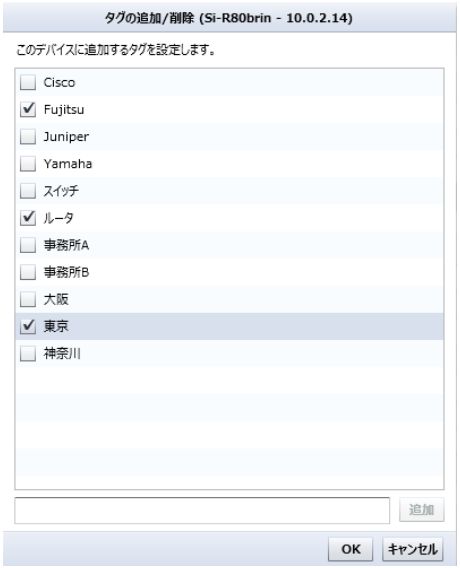


タグ用の名前を入力し、  ボタンを押します。

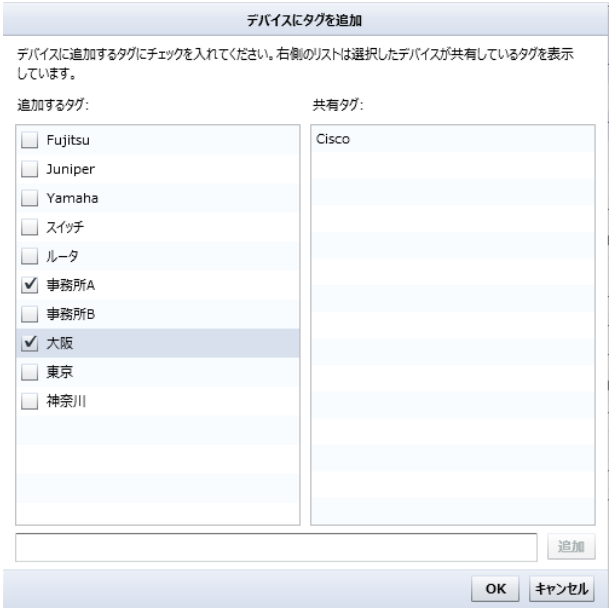
アイコン	説明
	タグを削除します。
	タグを編集します。 タグの名前をダブルクリックすることでも編集することができます。

デバイスビュー中のデバイスを選び、*デバイス→タグ付け*、あるいは*デバイス→タグ削除*ボタンを押します。

選択中のデバイスに関連付けるタグをオンにしてください。ここでオフにしたタグは、デバイスから削除されます。最後に OK ボタンを押し、保存してください。



複数のデバイスが選択されている場合には、各々に共有されているタグが表示されます。



9.4　ネイバー情報の表示

netLD は、ネイバー情報を表示することができます。*デバイス→ネイバー表示*を開いてください。

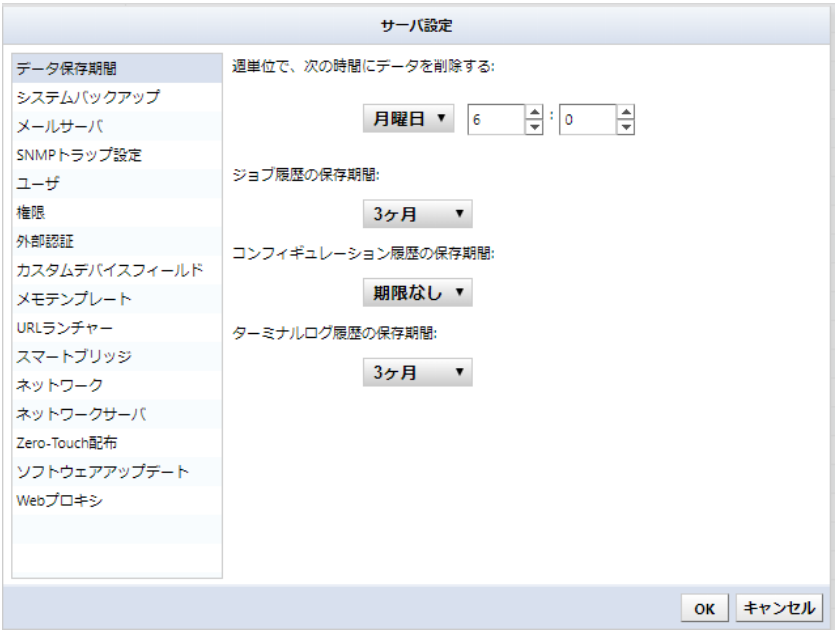
新しいタブがステータスペインに表示されます。

9.5　サーバ設定

この節では、サーバ設定ウィンドウ(設定ウィンドウ)で変更可能な様々な設定について解説します。この設定画面を出すためには、右上グローバルメニューの設定ボタンを押してください。

9.5.1　データ保存期間

netLD は、GUI で設定できるすべての設定データを常に保存します。しかし、長く運用を続けていると、データベースの大きさが肥大化してしまいます。この問題を解決するためには、データの保存期間を設定します。設定には、データ保存期間メニューを開きます。



※現在使われている設定データだけは、指定された期間を超えても消えることはありません。

週単位で、次の時間にデータを削除する項目では、データを削除するタイミングを設定します。残りの項目は、タイトルのとおりです。

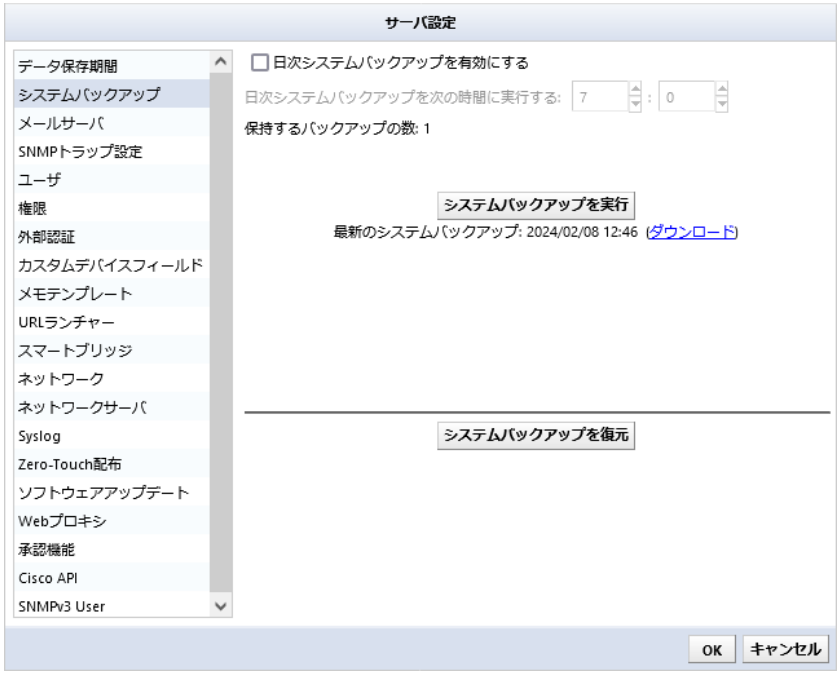
- コンフィギュレーション履歴の保存期間
- ターミナルログ履歴の保存期間
- ジョブ履歴の保存期間

9.5.2　システムバックアップ

netLD は、自身でそのデータをバックアップ・復元する機能をもっています。このバックアップも、スケジュールし自動化することができます。

9.5.2.1　システムバックアップを実行

システムバックアップ設定では、以下のような内容を変更することができます。リビジョン 20240131.0729 以降では、ローカルに保存されるシステムバックアップの数は「1」に制限されます。



項目	説明
日次システムバックアップを有効にする	オンにすると、バックアップスケジュールが有効になります。
日次システムバックアップを次の時間に実行する	システムバックアップを実行する時刻を指定します。
保持するバックアップの数	保存しておくバックアップの数を指定します。（1、7、14、30）
システムバックアップを実行	システムバックアップを実行します。
最新のシステムバックアップ	最後のバックアップが行われた時刻を表示します。
システムバックアップを復元	システムバックアップを復元します。

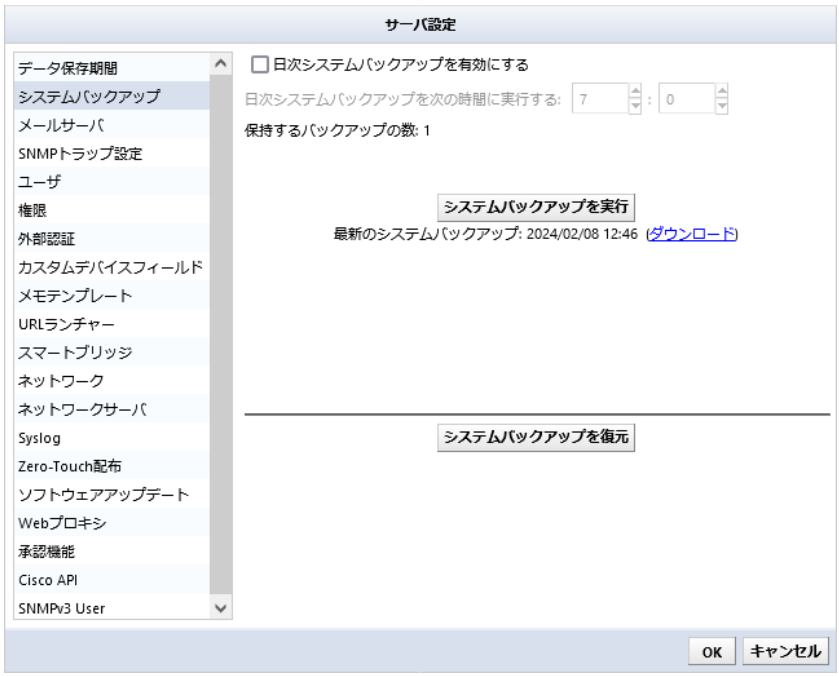
システムバックアップのファイル名は「backup_YYYY-MM-DD.zip」形式になります。

※ YYYY-MM-DD はシステムバックアップ実行時の協定世界時(UTC)の年月日を表します。また、システムバックアップの実行回数によって、ファイル名の末尾に「.1」などの枝番が付く場合があります。

（例）ファイル名: 「backup_2019-01-23.1.zip」

9.5.2.2　システムバックアップを復元

復元は同じリビジョンのデータでなければ成功しないことに注意してください。また、netLD をアップデートすると、バックアップデータも最新リビジョンに対応するようアップデートされることに注意してください。したがって、アップデート後のバックアップデータをアップデートされていない netLD に移し替えることは推奨されません。



「システムバックアップを復元」を選択し、バックアップデータファイルを選択し実行してください。復元実行後は自動的にサービスが再起動されます。

システムバックアップファイルの復元は admin のみ実行可能です。

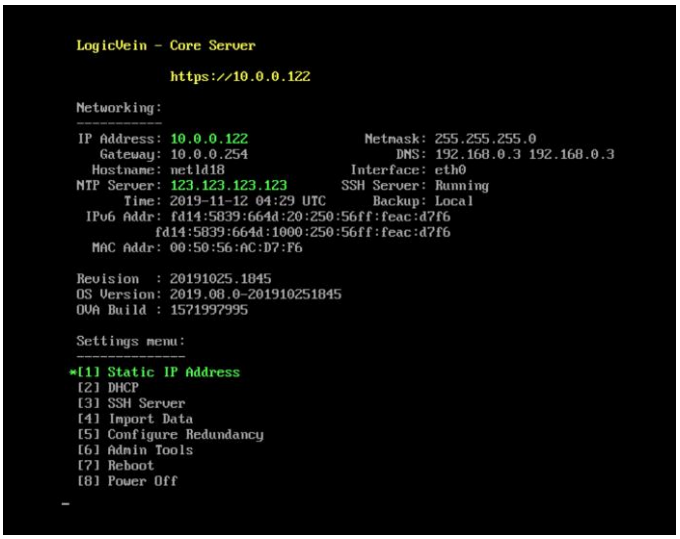
ファイル選択時には正しいシステムバックアップファイルを選択するようにしてください。誤ったファイルを復元すると、netLD が起動しなくなる恐れがあります。

9.5.2.3　外部ストレージに保存する

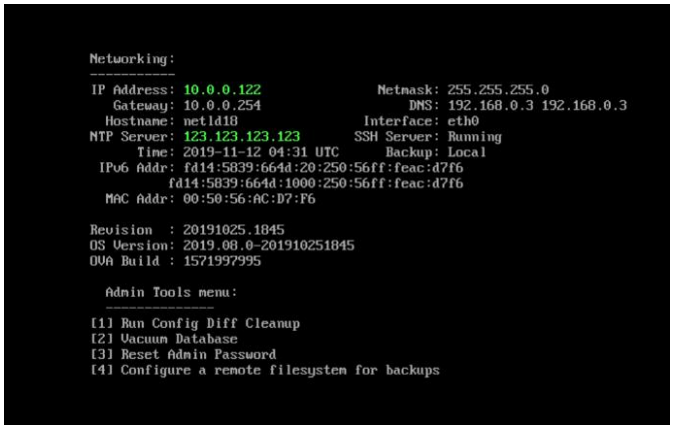
通常、netLD はシステムバックアップを netLD 内のディレクトリに保存します。ただし、設定を変更して、バックアップデータを外部ストレージに保存することも可能です。

外部ストレージを有効にするには、netLD のコンソール画面から設定を行います。コンソール画面での操作は、すべてキーボードのみで行います。

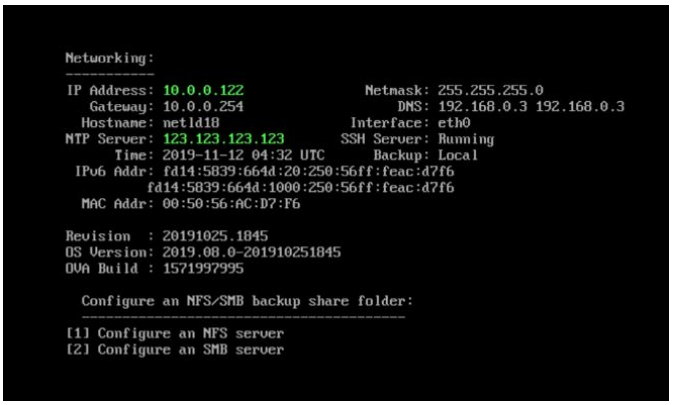
1. キーボードにて「6」を押します。



2. キーボードにて「4」を押します。



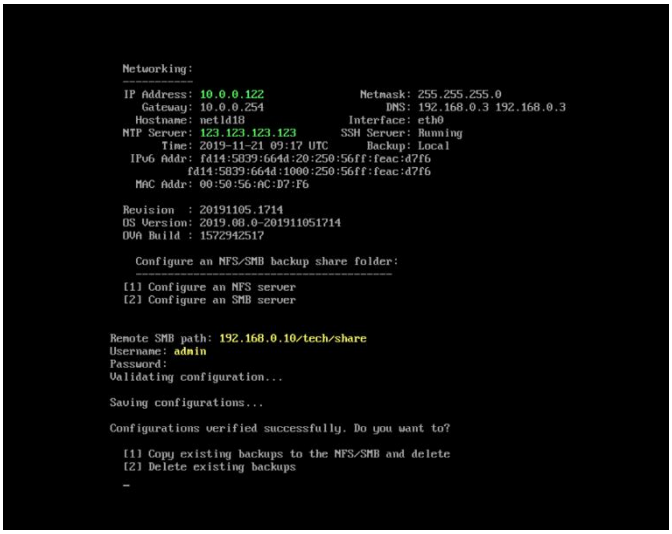
3. サーバの種類を選択します。



4. 必要な情報を入力し、エンターキーを押します。

項目	説明
Remote NFS/SMB path	ネットワークパス/IP アドレス
Username	サーバに設定しているユーザ名
Password	サーバに設定しているパスワード

5. 以下を選択します。

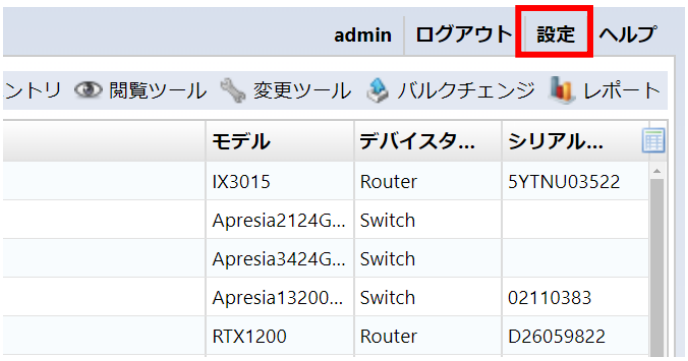


項目	説明
[1] Copy existing backuos to the NFS/SMB and delete	既存のバックアップを NFS/SMB にコピーしてから削除する
[2] Delete existing backups	既存のバックアップを削除する

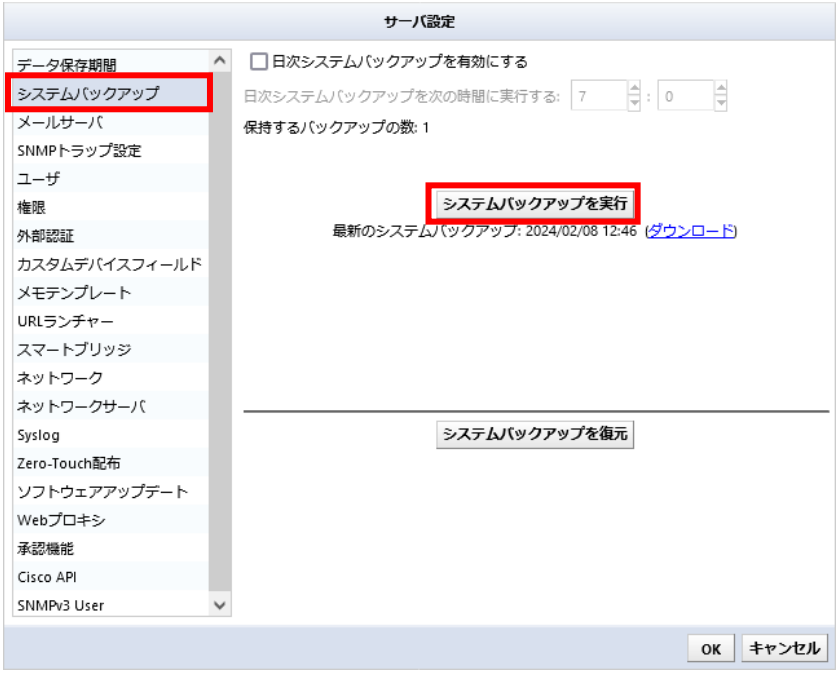
コンソール画面の設定はこれで終了です。

※セットアップが正常に行われると、自動的に再起動が行われます。

6. netLD の GUI 画面に移動し、「設定」をクリックします。



7. 「システムバックアップ」を選択し、「システムバックアップを実行」を押します。



外部システムにバックアップが保存されます。

9.5.2.4 システムバックアップを ZIP ファイルにする

システムバックアップを外部ストレージに保存している場合は、手動で ZIP ファイルを作成する必要があります。

1. バックアップフォルダを開きます。フォルダ名は「backup_YYYY¥MM¥DD」の形式になっています。
2. 次の 3 つのファイル/フォルダを 1 つの ZIP ファイルにまとめます。
   - pgsql（フォルダ）
   - complete（ファイル）
   - version.txt（ファイル）

9.5.3　メールサーバ機能

SMTP サーバを設定すれば、netLD が E-mail で通知を行えるようになります。

項目	説明
メールサーバのホスト名または IP アドレス	外部 SMTP サーバのアドレスです。
差出人 e メールアドレス	受信した側に表示される送信者アドレスです。
差出人名	受信した側に表示される送信者名です。
サーバ認証あり	対象 SMTP サーバに認証があるかどうかを指定します。
SMTPS を有効にする	SMTPS を使用する場合に
自動的に STARTTLS 通信を更新する	自動で TLS または SSL を使用して安全な接続にアップグレードします。
メールサーバのユーザ名	SMTP サーバにログインするユーザ名を指定します。
メールサーバのパスワード	SMTP サーバにログインするパスワードを指定します。
デフォルトの e メール言語	日本語か英語を選択します。
デフォルトの e メールタイムゾーン	タイムゾーンを選択します。
ルート証明書	メールサーバが証明書を必要とする場合は、[選択]からルート証明書(*.pem) を選択します。

9.5.4　外部認証機能

netLD で外部認証を構成すると、認証サーバを利用して製品にログインできるようになります。これにより、事前に netLD を使用するすべてのユーザアカウントを作成する必要がなくなります。また、認証サーバからグループの情報を取得して、製品権限やネットワーク閲覧制限を自動的に割り当てることもできます。

9.5.4.1　RADIUS 連携

RADIUS サーバに Access-Request を送信して認証を行います。RADIUS サーバと連携する為には Access-Accept に Filter-Id をつけて送信するように設定する必要があります。

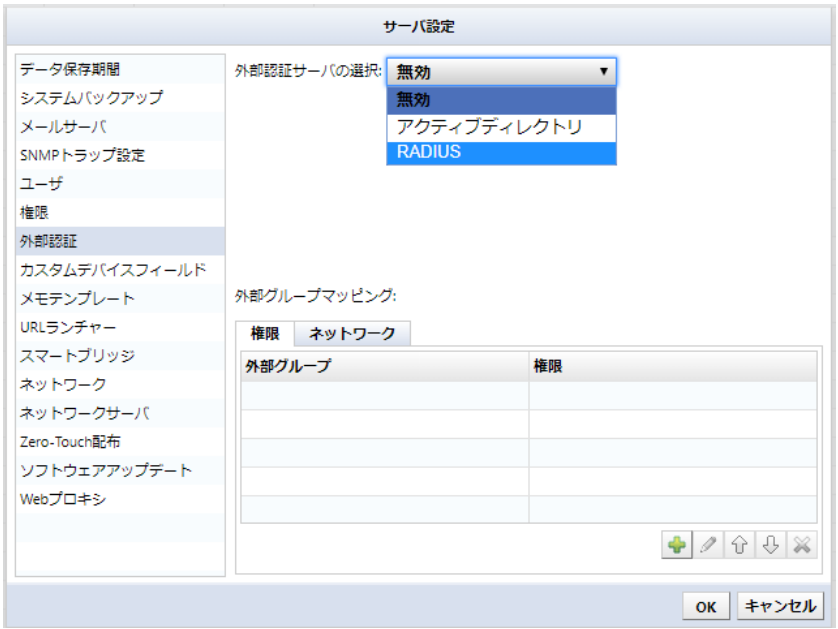
以下は FreeRADIUS のユーザ設定のサンプルです。

```
LogicVein Cleartext-Password: = "password"
Filter-Id += "GROUP"
```

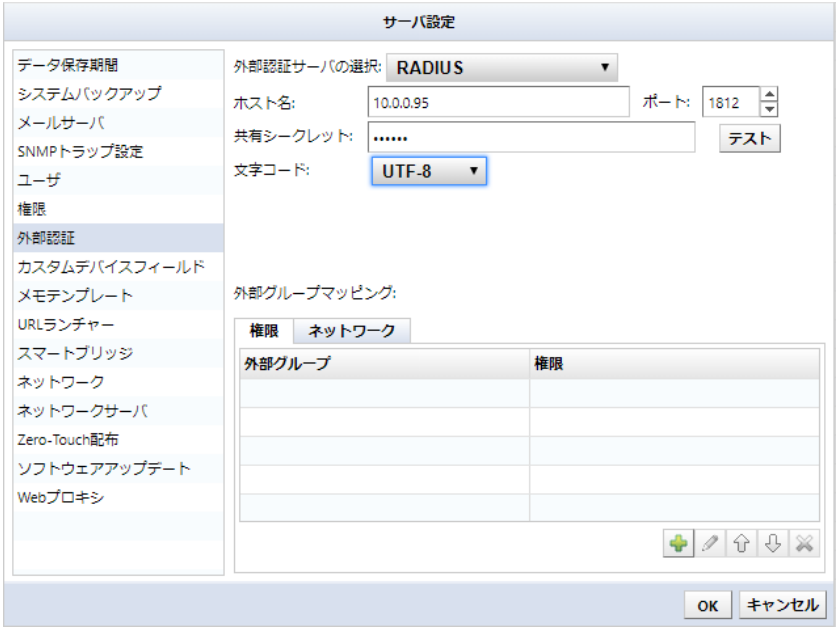
この設定では、netLD からユーザ名が「LogicVein」、パスワードが「password」の Access-Request を受信した場合、Filter-Id をセットして Access-Accept を送信します。Filter-Id は認証されたユーザが所属するグループとして使用されます。

【設定手順】

3. netLD で RADIUS サーバと連携する為に、設定ウィンドウ→外部認証で設定します。
4. 外部認証サーバの選択を無効から「RADIUS」に変更します。

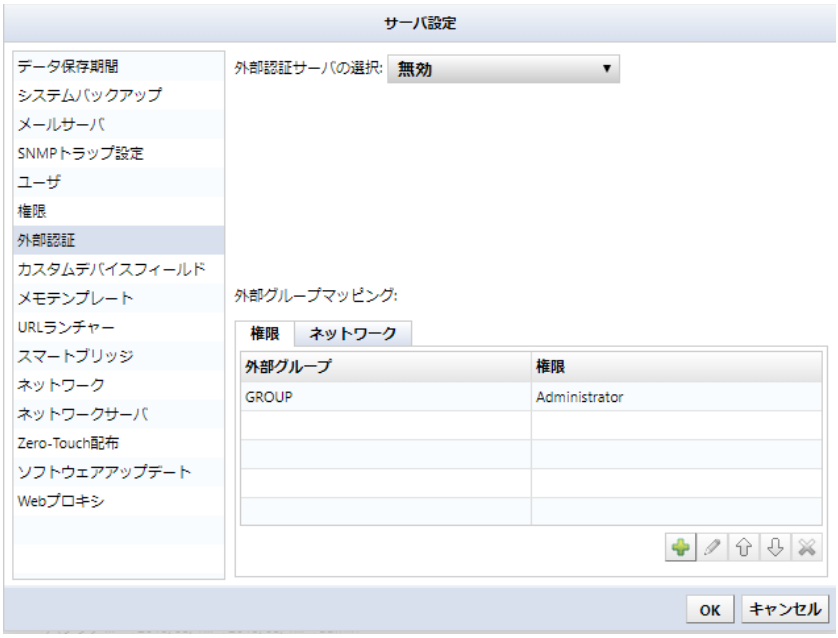


5. RADIUS サーバの IP アドレス（またはホスト名）と共有シークレットを設定します。

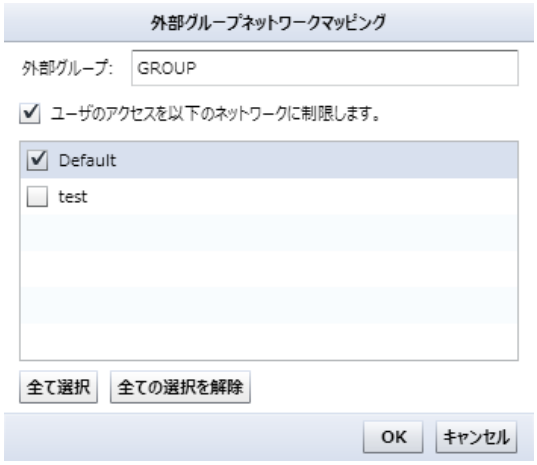


6. 外部グループマッピングの権限を設定します。  から新規追加します。
7. RADIUS サーバの Filter-Id に設定されているグループを外部グループに入力し割り当てる権限を選択します。

8. 外部グループマッピングのネットワークを設定します。  から新規追加します。



9. 権限と同様に RADIUS サーバの Filter-Id に設定されているグループを外部グループに入力し、閲覧できるネットワークを選択します。チェックがあるネットワークを閲覧する事ができます。



10. 設定後、テストからユーザ名とパスワードを入力し、テストをクリックすると RADIUS サーバとの連携を確認することができます。問題がなければ「認証が成功しました」と表示されます。

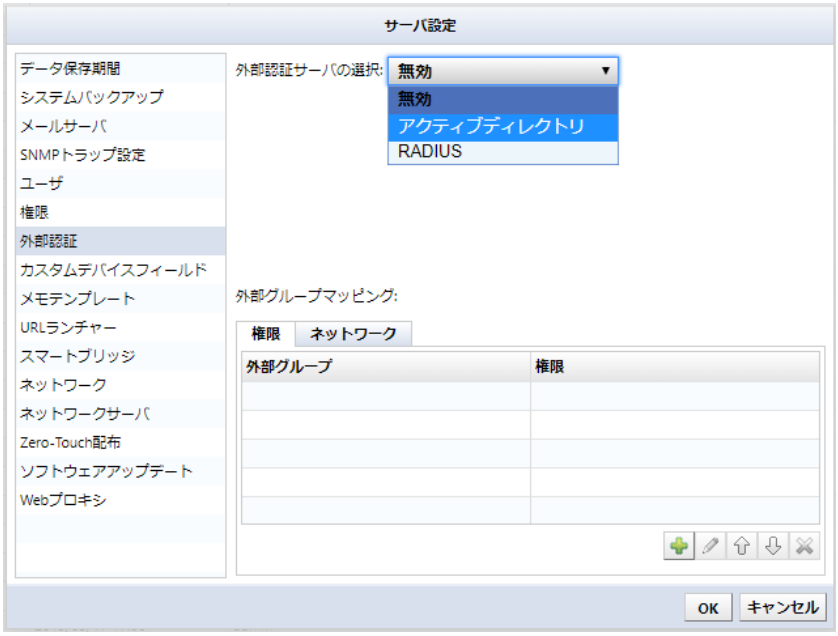
以上で設定が完了です。閉じるをクリックしサーバ設定を保存後、ログアウトし RADIUS サーバに設定されているユーザでログインします。

9.5.4.2 Active Directory 連携

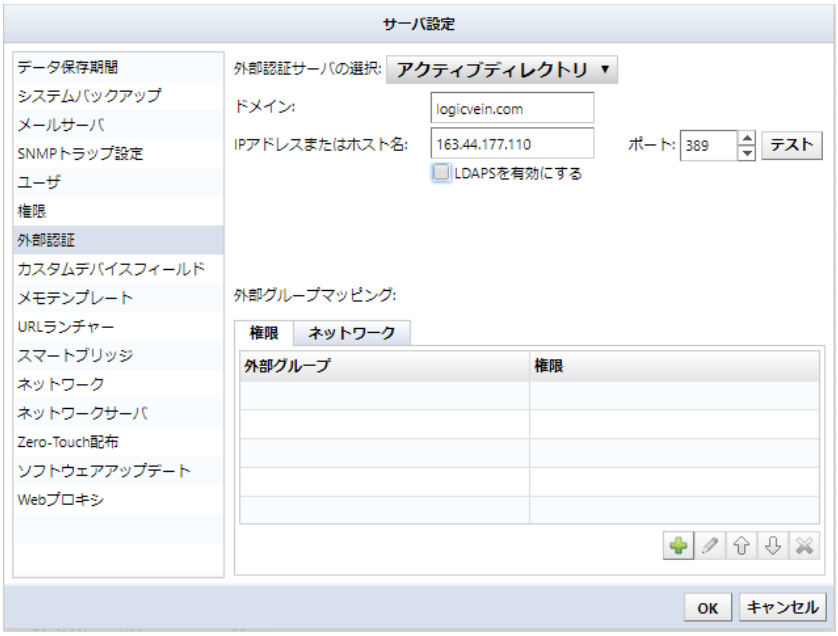
Active Directory サーバとの連携では登録されているユーザの所属するグループを使用して権限とネットワークを決定します。

【設定手順】

1. netLD で Active Directory サーバと連携する為に、設定→外部認証で設定します。
2. 外部認証サーバの選択を無効から「アクティブディレクトリ」に変更します。



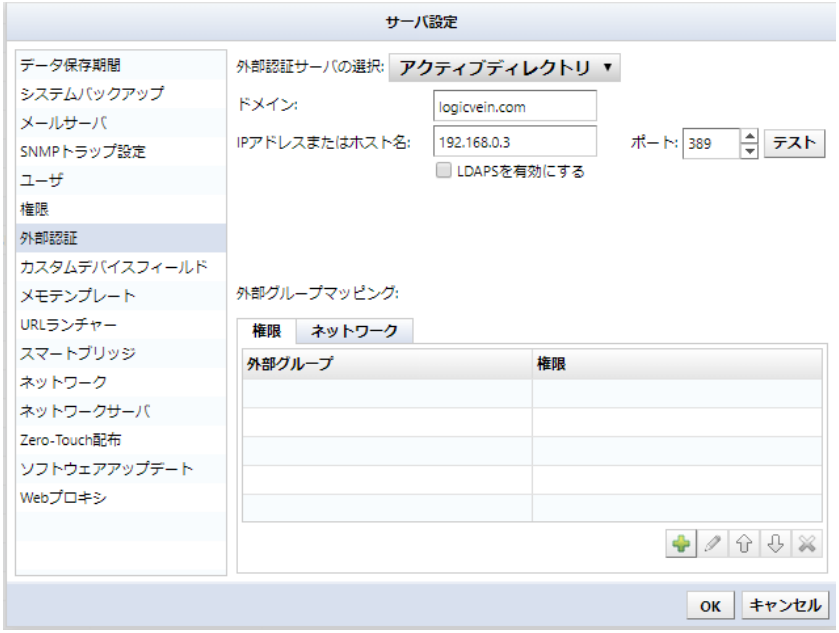
3. ドメイン名と Active Directory サーバの IP アドレス（またはホスト名）を以下のように設定します。



設定後、テストからユーザ名とパスワードを入力し、テストをクリックすると Active Directory サーバとの連携を確認することができます。

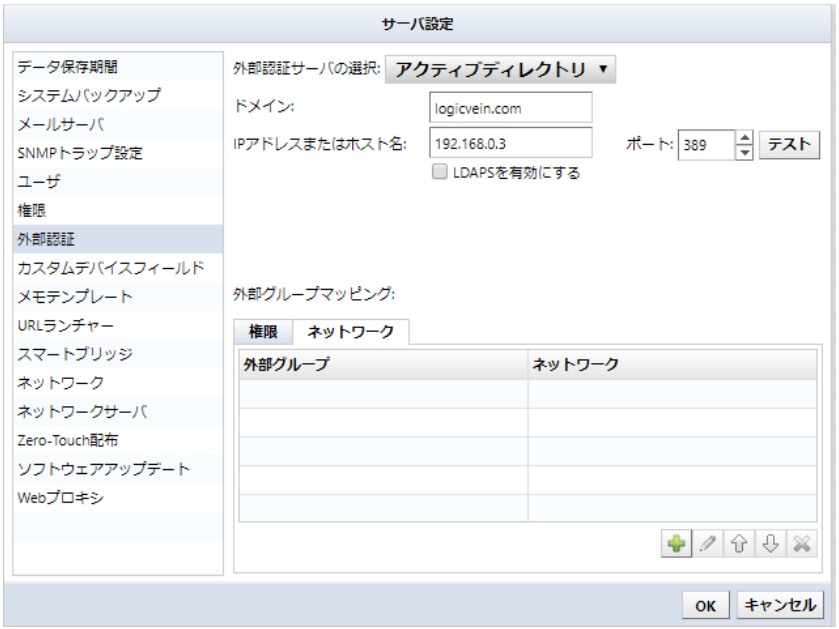
問題がなければ「認証が成功しました」と表示されます。

4. 外部グループマッピングの権限を設定します。  から新規追加します。

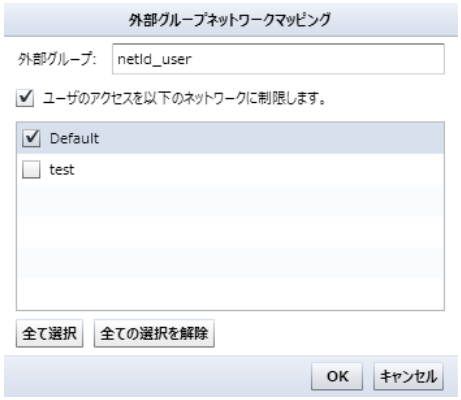


5. ユーザが所属しているグループを外部グループに入力し割り当てる権限を選択します。

6. 外部グループマッピングのネットワークを設定します。  から新規追加します。



7. 権限と同様にユーザが所属しているグループを外部グループに入力し閲覧できるネットワークを選択します。



設定後、テストからユーザ名とパスワードを入力し、テストをクリックすると Active Directory サーバとの連携を確認することができます。

問題がなければ「認証が成功しました」と表示されます。

以上で設定が完了です。OK をクリックしサーバ設定を保存後、ログアウトし Active Directory サーバに設定されているユーザでログインします。

9.5.4.3 SAML 連携

外部認証サービス（IdP）と連携した SAML 認証を構成することで、シングルサインオン（SSO）を実現できます。これにより、ユーザは IdP 経由で netLD にシームレスにログインできるようになります。

（1） Microsoft Entra ID 連携

【前提条件】

シングルサインオンを構成する前に、以下の条件を満たしていることを確認してください。

- 管理者権限で Microsoft Entra ID にサインインできること
- Microsoft Entra ID に連携対象のユーザおよびグループが存在すること
- netLD で設定を構成する権限(※)を持っていること
  - (※) Administrator 権限 または 「セキュリティの設定を許可する。」を有する権限

【手順】

(i) netLD で SAML を構成する

1. netLD にログインします。
2. ［設定］＞［外部認証］を開きます。
3. ［外部認証サーバの選択］から「SAML」を選択します。
4. ［コールバック URL］が netLD サーバの正しい URL であることを確認します。
   ※ コールバック URL の形式： https://[IP アドレスまたはホスト名]/auth
   ※ デフォルトでは、［ネットワークサーバ］＞［パブリック ホスト名/IP アドレス］の値を参照します。
5. ［SP メタデータ XML をダウンロード］リンクをクリックして、SP メタデータ XML ファイルをダウンロードします。
   ※ ファイル名: LogicVein-saml-sp-metadata.xml
   ※ ダウンロードしたファイルは、次の手順で利用します。

(ii) 新しいアプリケーションを作成

1. 「Microsoft Entra 管理センター」にサインインします。
2. ［ID］＞［アプリケーション］＞［エンタープライズ アプリケーション］を開きます。
3. ［新しいアプリケーション］メニューをクリックします。
4. ［独自のアプリケーションの作成］メニューをクリックします。
5. アプリの名前を設定し、［ギャラリーに見つからないその他のアプリケーションを統合します（ギャラリー以外)］を選択し、［作成］をクリックします。
6. ［管理］＞［シングル サインオン］を選択します。
7. ［シングル サインオン方式の選択］ページで、［SAML］を選択します。
8. ［SAML によるシングル サインオンのセットアップ］で、［メタデータ ファイルをアップロードする］をクリックし、先の手順でダウンロードした「LogicVein-saml-sp-metadata.xml」をアップロードし、［追加］をクリックします。

9. ［保存］をクリックします。
10. ［×］をクリックして編集画面を閉じます。
    ※ ［シングル サインオンを Test］のポップアップメッセージが表示された場合、「いいえ、後で test します」をクリックします。
11. ［属性とクレーム］セクションで［編集］をクリックします。
12. ［属性とクレーム］ページで、［グループ要求を追加する］を選択します。
13. ［セキュリティグループ］オプションを選択し、［ソース属性］で「グループ ID」を選択します。
14. ［保存］をクリックします。
15. ［×］をクリックして［属性とクレーム］ページを閉じます。

(iii) IdP メタデータを取得

1. ［SAML 証明書］セクションで、［フェデレーション メタデータ XML］の［ダウンロード］をクリックします。
2. IdP メタデータ XML ファイルをダウンロードします。

(iv) netLD にアプリケーションを登録

1. netLD の［設定］>［外部認証］を開きます。
2. ［IdP メタデータ XML をアップロード］をクリックし、手順「(iii) IdP メタデータを取得」で作成した XML ファイルを選択します。
3. ［OK］をクリックし、［サーバ設定］を保存します。

(v) オブジェクト ID をメモ

1. 「Microsoft Entra 管理センター」に戻り、［管理］>［ユーザーとグループ］をクリックします。
2. ［ユーザーまたはグループの追加］をクリックします。
3. ［ユーザー］セクションの［選択されていません］をクリックします。
4. 一覧から、netLD へのログインを許可する必要があるユーザを選択します。
5. ［選択］をクリックします。
6. ［割り当て］をクリックして、ユーザーの割り当てを完了します。
7. 左側のペインで［ID］>［グループ］>［すべてのグループ］に移動します。
8. ThirdEye へのログインを許可するグループの［オブジェクト ID］をメモします。

(vi) 外部グループマッピングを構成する

1. ［設定］>［外部認証］を開きます。
2. ［外部グループマッピング］で、［+］をクリックします。
3. ［外部グループ］フィールドに、先の手順でメモした「オブジェクト ID」を入力し、［権限］に割り当てる権限を指定して、［OK］をクリックします。
4. ［OK］をクリックし、［サーバ設定］を保存します。

5. netLD のログアウトをクリックします。Microsoft のログインページに移動します。

(2) Okta 連携

【前提条件】

シングルサインオンを構成する前に、以下の条件を満たしていることを確認してください。

- **管理者権限で Okta ダッシュボードにサインインできること**
- **Okta に連携対象のユーザおよびグループが存在すること**
- **netLD で設定を構成する権限(※)を持っていること**
  - (※) Administrator 権限 または 「セキュリティの設定を許可する。」を有する権限

【手順】

(i) netLD で SAML を構成する

1. netLD にログインします。
2. ［設定］>［外部認証］を開きます。
3. ［外部認証サーバの選択］から「SAML」を選択します。
4. ［コールバック URL］がサーバの正しい URL であることを確認します。
   ※ デフォルトでは、［ネットワークサーバ］>［パブリック ホスト名/IP アドレス］の値を参照します。
5. ［SP 証明書をダウンロード］リンクをクリックして、SP 証明書ファイルをダウンロードします。
   ※ ファイル名: LogicVein-saml-sp-signing-certificate.crt
   ※ ダウンロードしたファイルは、次の手順で利用します。

(ii) 新しいアプリケーションを作成

1. Okta Admin Console で、［Applications］>［Applications］に移動します。
2. ［Create App Integration］をクリックします。
3. ［Sign-in method］として［SAML 2.0］を選択し、［Next］をクリックします。
4. ［App name］に任意の名前を入力し、［Next］をクリックします。
5. ［SAML Settings］の［General］セクションで、以下の項目を設定します。

項目	設定
Single sign-on URL	https://[IP アドレスまたはホスト名]/auth?client_name=SAML2Client
Audience URI (SP Entity ID)	https://[IP アドレスまたはホスト名]/auth
Application username	メール
Update application username on	作成・更新

6. ［Show Advanced Settings］をクリックします。
7. ［Signature Certificate］で［Browse files...］をクリックし、先の手順で netLD からダウンロードした SP 証明書を選択します。

   ※ ファイル名: LogicVein-saml-sp-signing-certificate.crt
8. 以下の項目を設定します。

項目	設定
Enable Single Logout	有効 「Allow application to initiate Single Logout」オプションにチェックを入れる
Single Logout URL	https://[IP アドレスまたはホスト名]
SP Issuer	https://[IP アドレスまたはホスト名]/auth

9. ［Attribute Statements (optional)］セクションで、次の 2 つの項目を追加します。

   ※ 1)

Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Name format	URI 参照
Value	user.email

   ※ 2)

Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Name format	URI 参照
Value	user.lastName

10. ［Group Attribute Statements (optional)］セクションで、次のように設定します。

Name	http://schemas.logicvein.com/ws/2024/05/identity/claims/groups
Name format	URI 参照
Filter	正規表現と一致
	.*

11. ［Next］をクリックします。
12. 「I'm an Okta customer adding an internal app」を選択します。
13. 「It's required to contact the vendor to enable SAML」を選択します。
14. ［Finish］をクリックします。

(iii) アプリケーションを利用するグループを割り当て

1. アプリケーションの［Assignments］タブを選択します。
2. ［Assign］>［Assign to Groups］を選択します。
3. 割り当てるグループを見つけて、［Assign］ボタンをクリックします。
4. ［Done］をクリックします。

(iv) IdP メタデータを取得

1. ［Sign On］タブを選択します。
2. ［Settings］で［Metadata URL］の URL をコピーします。
3. ブラウザの新しいタブを開き、アドレスバーに URL を貼り付けてアクセスします。
4. メタデータページを右クリックし、［名前を付けて保存...］を選択します。
   ※ メタデータを .xml ファイル として保存します。
   ※ ダウンロードしたファイルは、次の手順で利用します。

(v) netLD にアプリケーションを登録

1. netLD の［設定］>［外部認証］を開きます。
2. ［IdP メタデータ XML をアップロード］をクリックし、手順「(iv) IdP メタデータを取得」で作成した XML ファイルを選択します。

(vi) 外部グループマッピングを構成する

1. ［設定］>［外部認証］を開きます。
2. ［外部グループマッピング］で、［+］をクリックします。
3. ［外部グループ］フィールドに Okta グループ を入力し、［権限］に割り当てる権限を指定して［OK］をクリックします。
4. ［OK］をクリックします。

(vii) netLD にログイン

Okta のユーザで netLD にログインします。
「(2) Okta 連携」に記載された設定が完了後、netLD にアクセスすると Okta のサインオン画面が表示されます。

9.5.4.4 SAML 認証を設定したあとにローカル認証を使用する方法

SAML 認証の設定完了後、netLD の製品ページにアクセスすると、連携先のサインインページが表示されます。SAML 認証ではなく、ローカル認証を使用して製品にログインする場合は、URL の末尾に変数 「/?forceLoginPage=true」 を追加してアクセスします。

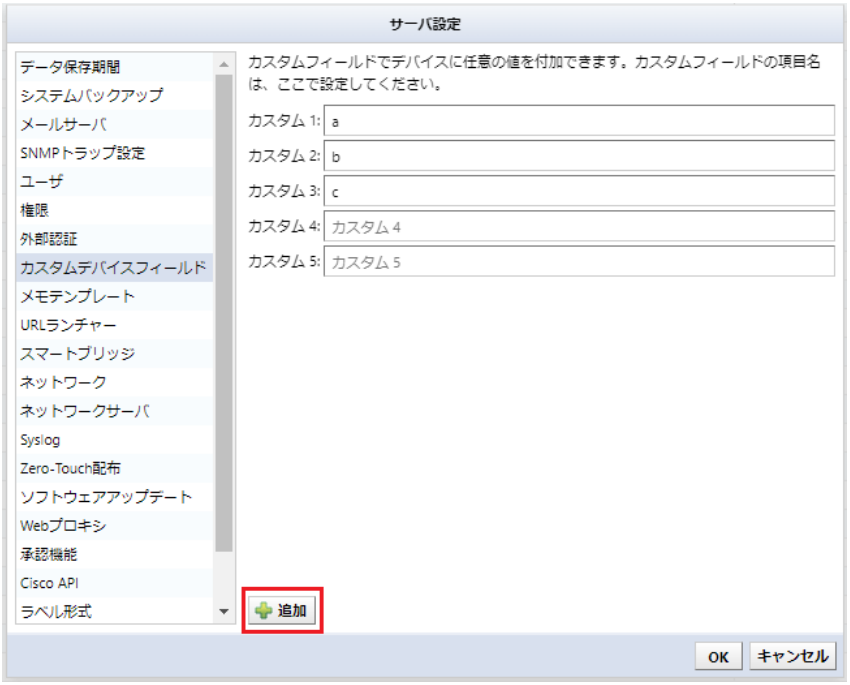
```
https://[IP アドレスまたはホスト名]/?forceLoginPage=true
```

変数を付け加えた URL を開くと、製品のログインページが表示されます。admin などのローカルアカウントでログインできます。

9.5.5　カスタムデバイスフィールド

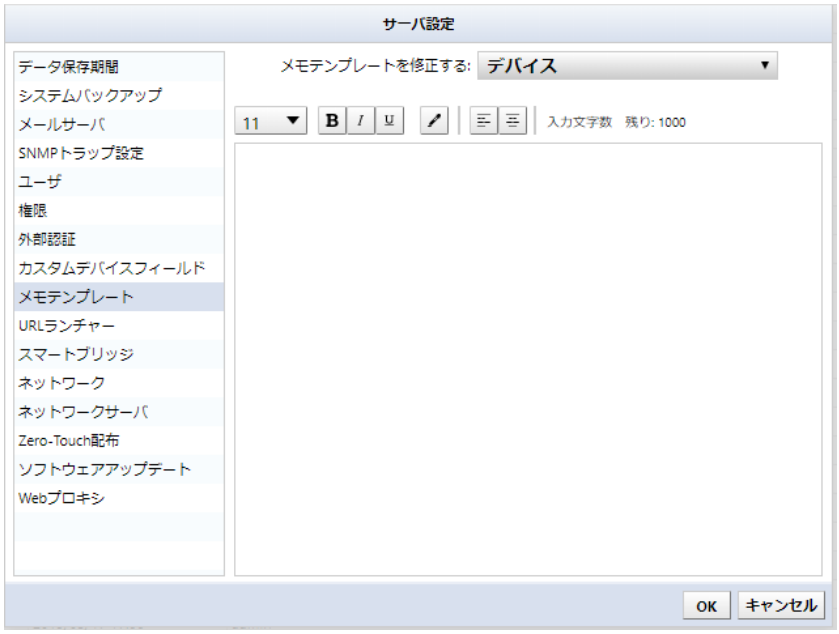
ここでは、インベントリ情報に任意のカラムを追加することができ、またカスタムフィールドのカラム名を変更できます。 値の入力方法については 「デバイス」をご参照ください。

※ 一度追加したカスタムデバイスフィールドは削除できません。

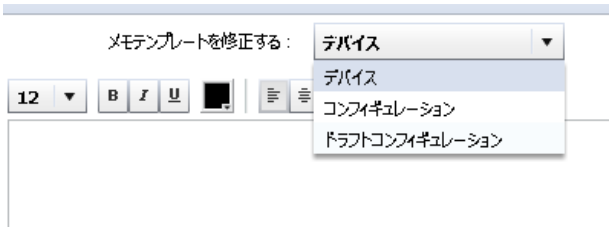


9.5.6　デフォルトのメモテンプレートの変更

ここでは、デバイスビューや各コンフィグに設定できるメモのテンプレートを作成することができます。



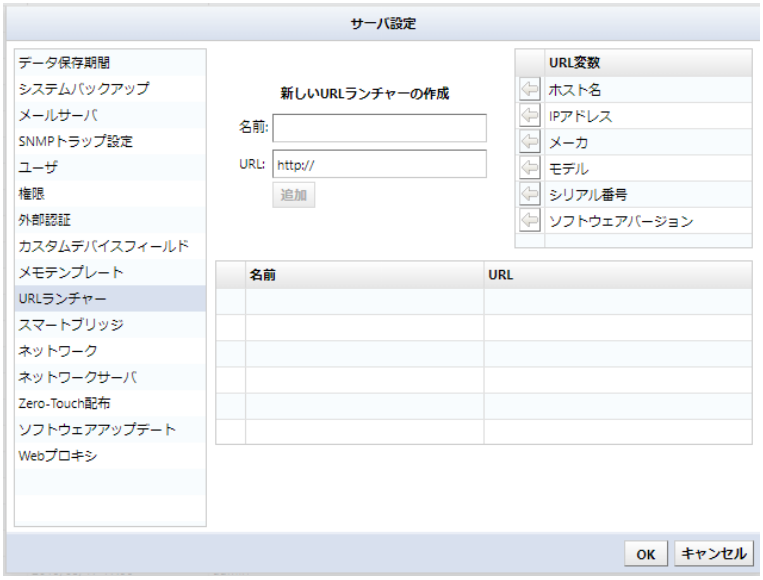
テンプレートはデバイス/コンフィギュレーション/ドラフトコンフィギュレーションの 3 種類を作成することができます。



9.5.7 URL ランチャー

デバイスビューの右クリックメニューに、任意の URL へのショートカットを作成できます。例えば、特定のデバイスの Web コンソールに接続したい場合に便利です。

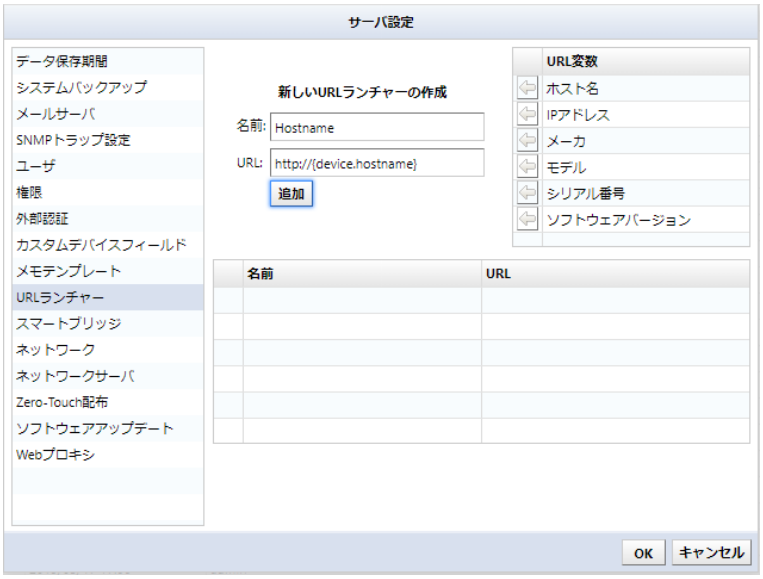
設定は、サーバ設定ウィンドウ→URL ランチャーから行います。



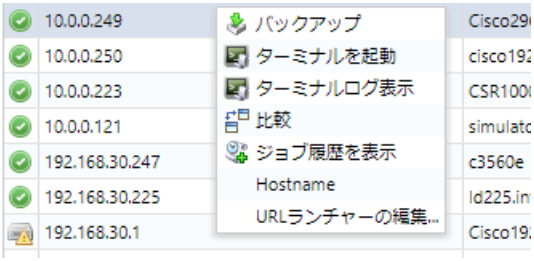
URL ランチャーを作成するには、まず名前を入力します。この名前は、デバイスビューの右クリックメニューに表示されます。次に、URL を入力します。URL には右側の「URL 変数」にある特定のパターンを変数として含めることができます。URL 変数を使用すると、URL ランチャー実行時に対象デバイスの実際の値が変数部分に代入されます。URL 変数を利用するには、矢印ボタンをクリックして変数を URL に追加します。

URL 変数「ホスト名」を使用した URL ランチャーの作成例を以下に示します。

「Hostname」と名前を指定し、URL 変数「ホスト名」の矢印ボタンをクリックすると、{device.hostname} という変数が URL に挿入されます。



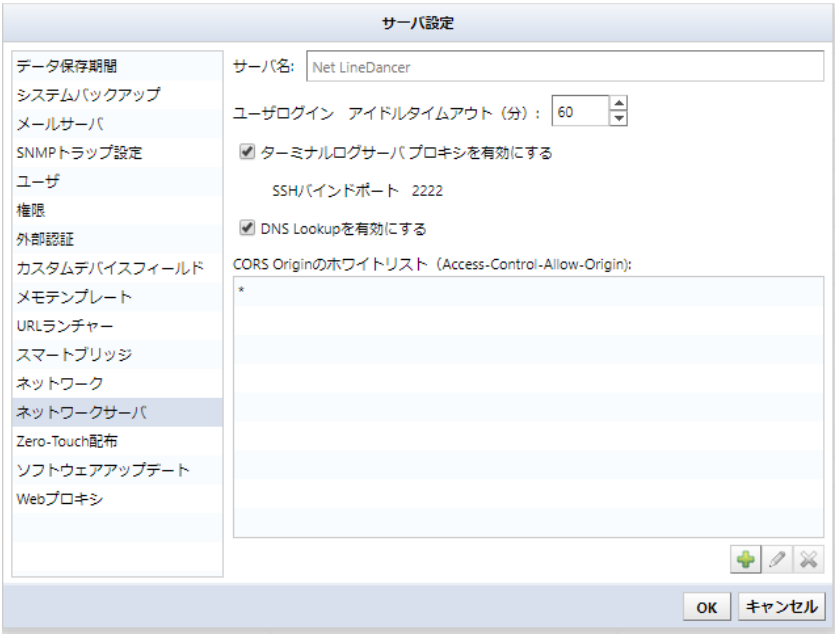
追加後、作成した URL ランチャー「Hostname」がデバイスビューの右クリックメニューに表示されます。



このメニューをクリックすると、対象デバイスの情報を変数に代入した URL が自動的に生成され、その URL にブラウザでアクセスできるようになります。例えば、デバイスのホスト名が「www.lvi.co.jp」の場合、この URL ランチャーメニューをクリックすることで、http://www.lvi.co.jp に簡単にアクセスできます。

9.5.8　ネットワークサーバ

ネットワークサーバ管理メニューでは、無操作時に自動でログアウトする時間やサーバのプライマリ IP アドレスなどを設定することができます。



9.5.8.1　ログインアイドルタイムアウト

ログインアイドルタイムアウトは、間違えて放置してしまった画面を権限が持たないものが無許可で操作しないよう、無操作時に netLD GUI から自動でログアウトする機能です。タイムアウト時間はデフォルトで 30 分ですが、この設定画面から値を変更することができます。

この機能を無効にすることはできません。これは、無効にすることが明らかにセキュリティ上好ましくないからです。もし担当者がちょっと席を外した隙に何者かが画面を操作し、ネットワーク全体のコンフィグデータを詐取したとしたら、これは大変なシステム不正となります。

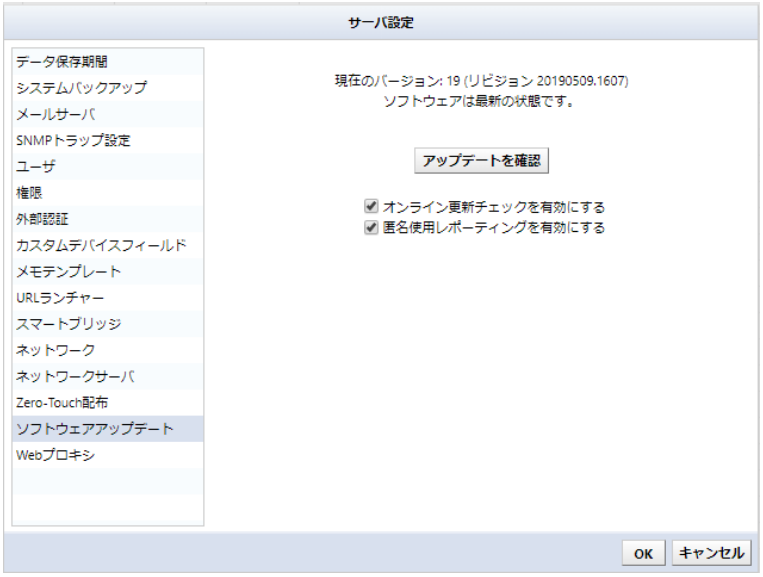
9.5.8.2　DNS Lookup を有効にする

ネットワークサーバ管理メニューの DNS Lookup を有効にするにチェックを入れる事で、デバイスのホスト名が DNS 逆引きでの表示となります。

DNS Lookup のチェックを外す事で機器に設定してあるホスト名表記となります。
※設定を変更した後、デバイスのバックアップを行う事でホスト名表記となります。

9.5.9　ソフトウェアアップデート

netLD はアップデートを自動で検知し、変更があれば通知します。この設定画面では、手動でこの変更通知を更新することができ、アップデートがあれば更新を手動で行うことができます。更新には、新たなアダプタへの対応やマニュアルの更新も含みます。自動アップデート機能を用いるには、インターネット接続が必要です。



アップデート通知は通常画面上に表示されます。

通知されたアップデートを実行するには、「アップデートをインストール」ボタンをクリックします。

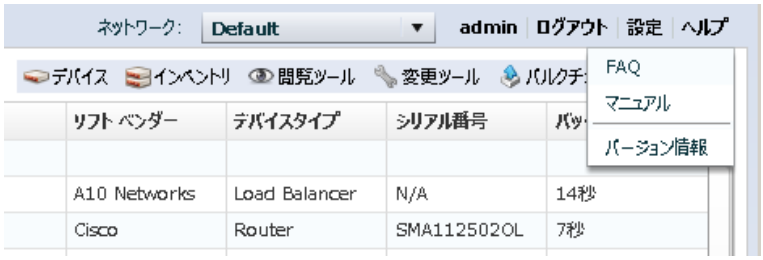
「OK」ボタンを押して続けます。

ダウンロードが自動で始まります。

アップデートが完了すると、netLD サービスは自動で再起動し、新たなログイン画面が現れます。

9.6 ヘルプ

ヘルプメニューは、ログをカスタマーサポートに送信することや、マニュアルや FAQ を閲覧することに用います。



項目	説明
FAQ	ブラウザで LogicVein のカスタマーポータルの FAQ コミュニティを開きます。
マニュアル	netLD の製品マニュアルを開きます。
バージョン情報	バージョン情報では、製品のリビジョンやライセンスを確認できます。また、デバッグに役立つ機能を実行することもできます。デバッグ機能を使用するには、admin ユーザとして netLD にログインする必要があります。

項目	説明
リビジョン	現在稼働している netLD のリビジョンを確認できます。
エンドユーザライセンス契約（EULA）	EULA の内容を確認できます。
ライセンシー	ライセンスの所有者。
ライセンス有効期限	ライセンスの有効期限。

項目	説明
	基本的には「永久」と表示されますが、年間ライセンスを使用している場合には期限が表示されます。
サポート有効期限	契約しているサポートの有効期限。
ノード	現在使用できるノードと使用しているノード数。 構成は「使用上限ノード数（現在使用中のノード数）」です。
シリアル番号	使用中のシリアル番号。
ライセンス更新	サポート有効期限の更新したり、管理ノード数を変更した場合は、ここからライセンスを更新できます。更新すると、サービスが再起動することがあります。詳しくは、9.6.3 ライセンスアップデートを参照してください。
アダプタ診断設定	コンフィグバックアップ等が失敗する際に詳細なログを出力する設定を行います。 詳しくは、9.6.1 アダプタ診断ログを参照してください。
ログ送信	netLD の各種ログファイルを support@lvi.co.jp に送信することができます。 詳しくは、9.6.2 ログ送信を参照してください。

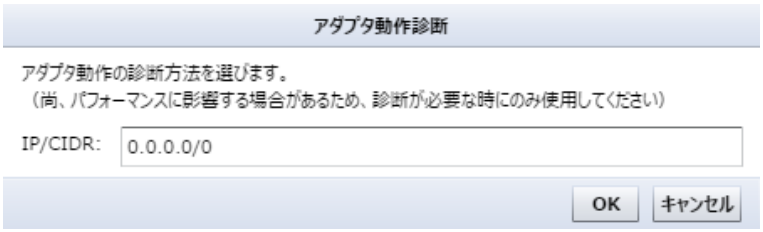
9.6.1 アダプタ診断ログ

アダプタ診断ログとは、デバイスに対する製品動作を取得するためのデバッグログ機能です。この機能は、有効にしてから 5 分後に自動的にオフになります。

アダプタ診断ログを収集するには、次の手順に従ってください。

1. ［ヘルプ］→［バージョン情報］をクリックします。
2. ［アダプタ診断設定］をクリックします。

3. デバッグ対象となるデバイスの IP アドレスを入力し、［OK］をクリックします。



※ 対象デバイスが複数ある場合は、上図のように CIDR 表記を使用してネットワークを指定できます。ネットワーク全体を対象にデバッグを実行する場合は、「0.0.0.0/0」と指定できます。

4. デバッグ対象の操作（バックアップやツールなど）を実行します。

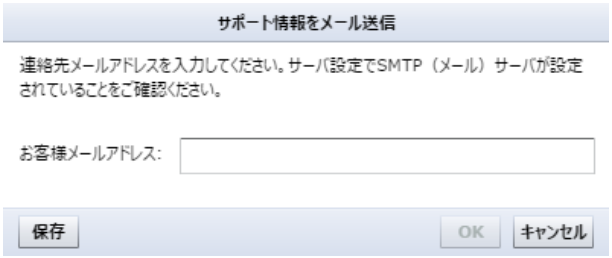
9.6.2　ログ送信

アダプタ診断で取得したログは、直接ロジックベインカスタマーサポートに送信することができます。

ヘルプからバージョン情報を開き、ログ送信を押します。

送信元となるメールアドレスを入力し、OK を押します。

（宛先は support@lvi.co.jp で固定となります。）



以上の操作で自動的に必要なログがロジックベインカスタマーサポートに送信されます。最初に HTTP を使用して弊社サーバに送信し、失敗した場合にはサーバ設定の SMTP サーバを使用してログを送信します。

SMTP サーバを使用する場合は、9.5.3 メールサーバ機能を参照し設定を行ってください。

また、ログをログ送信画面からローカルに保存できます。ご使用されている環境がインターネット接続されていない場合などにはログをローカルに保存しメール送信できる端末から保存したログを弊社にお送りください。

9.6.3　ライセンスアップデート

GUI 上からライセンスのアップデートができます。

ヘルプからバージョン情報を開きます。

「ライセンス更新」をクリックするとライセンス更新が開始されますが、インターネットに接続されている環境とされていない環境で操作が異なります。

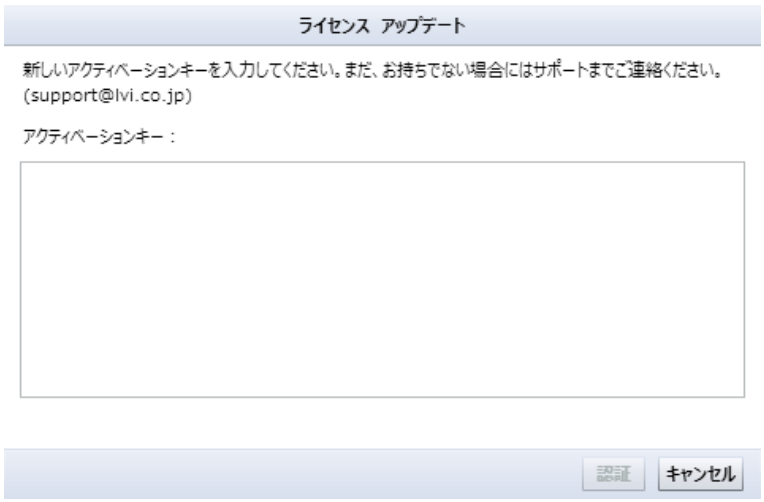
9.6.3.1　インターネットに接続されている環境

ライセンス更新をクリックすると弊社アクティベーションサーバと通信し、ライセンスがアップデートされます。

OK をクリックしライセンスを更新します。更新後は自動でサービスが再起動しログイン画面に戻ります。

9.6.3.2　インターネットに接続されていない環境

ライセンス更新をクリックするとアクティベーションキーの入力画面が表示されます。



「ライセンス認証」と同様にカスタマーサポートより取得したアクティベーションキーを入力し、認証をクリックしてください。適用後はインターネットに接続されている環境と同様にサービスが再起動しログイン画面に戻ります。

9.7　その他の機能

ここでは、これまでのカテゴリに分類できない機能の使用方法を解説します。

9.7.1　ブラウザ用セキュリティ証明書の設定

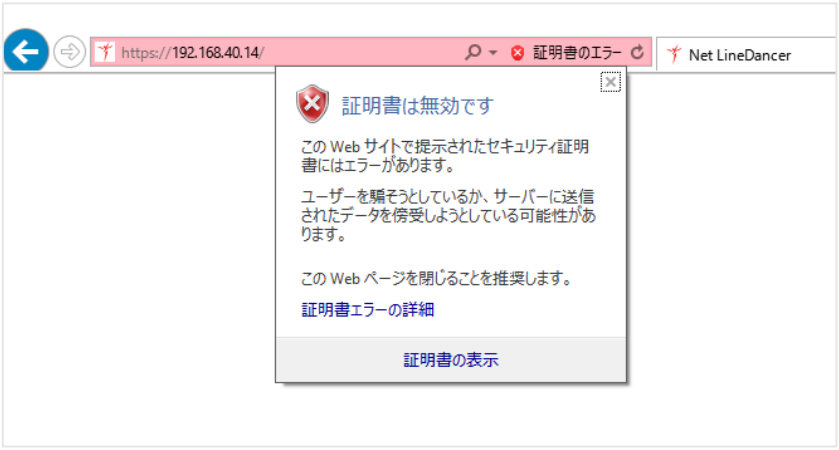
netLD では、HTTPS を使用してサーバに接続し、画面操作を行なうため、サーバアクセス時にセキュリティ証明書の警告画面が表示される場合があります。警告画面は無視しても全く問題ありませんし、完全に安全です。ですが、必要な設定を行えば、警告画面を表示しないようにすることもできます。ここでは、そのための手順(SSL 証明書の発行とインストールの手順)をご説明します。

設定はブラウザ上で行います。今回説明に用いるブラウザは Internet Explorer に限定していますが、Google Chrome や Mozilla Firefox などの他のブラウザでも似た手順で同様の設定を行うことができます。

9.7.1.1　SSL 認証書のインストール

Internet Explorer を「管理者として実行」から開き、netLD サーバの HTTPS のアドレスを開いてください。このサイトの閲覧を続行する(推奨されません)を押してください。

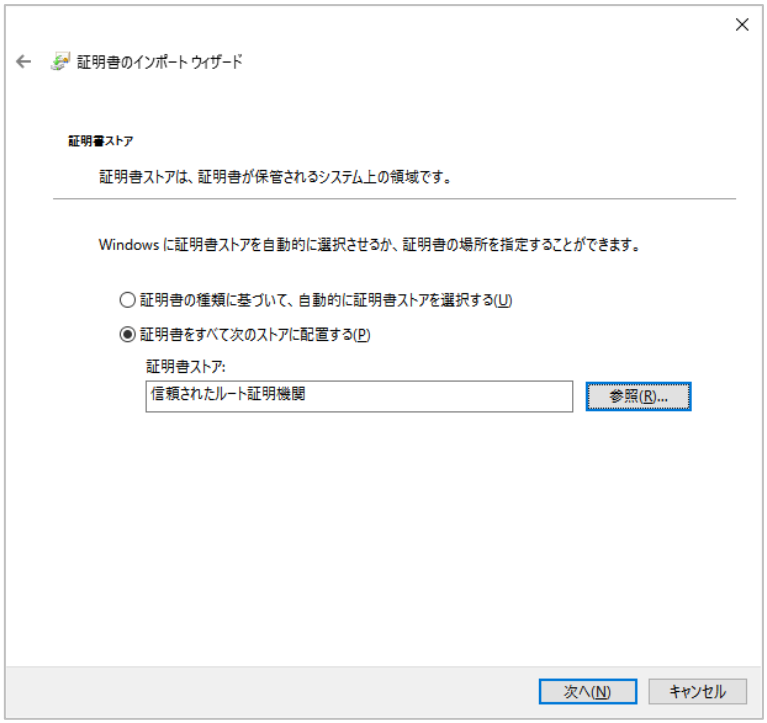
アドレスバー付近に現れる証明書のエラーを押し、エラーメッセージを開いてください。証明書は無効ですと書かれたポップアップが開きます。ここで明書の表示と書かれたラベルをクリックしてください。



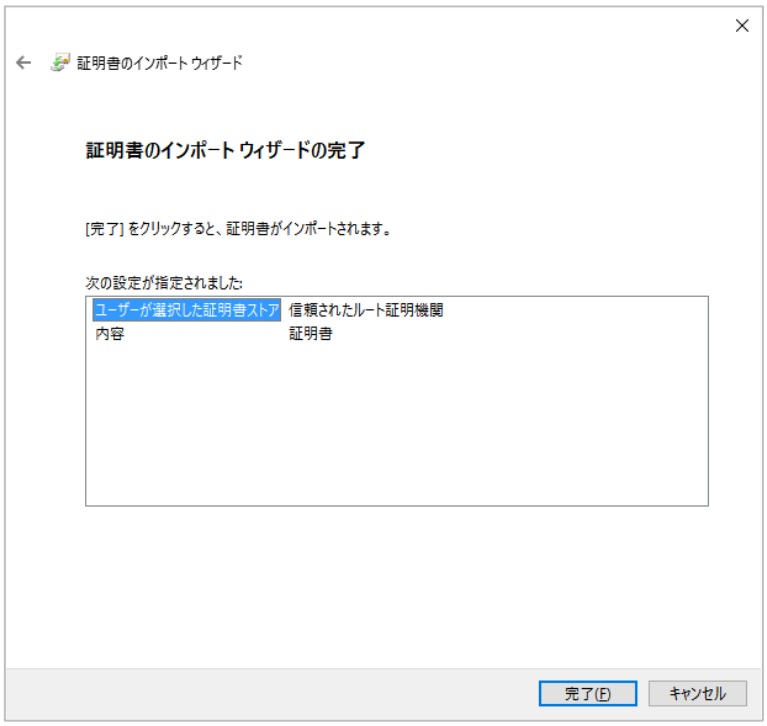
1. 証明書のインストール(I)ボタンを押してください。

2. 「次へ」ボタンを押してください。

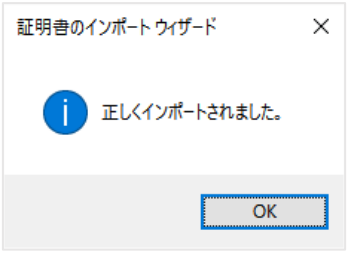
3. 証明書をすべて次のストアに配置するを押し、ボタンを押してください。



4. 「完了」 ボタンを押してください。



5. OK ボタンをクリックしてウィザードを終了します。



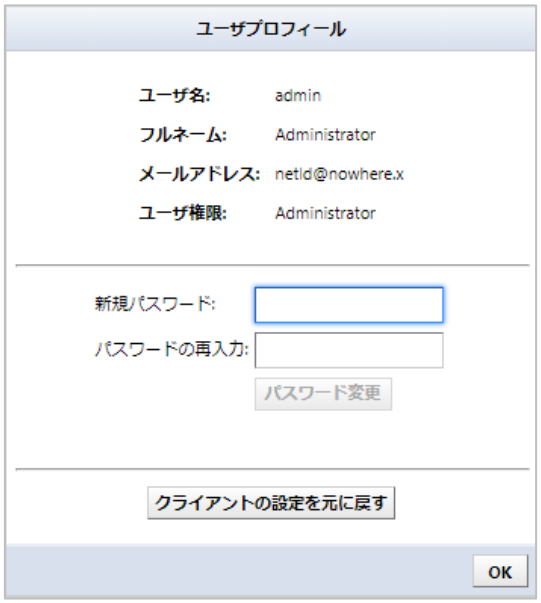
6. OK ボタンを押して証明書画面を閉じます。

Internet Explorer を再起動し、 netLD GUI に再びアクセスして、 セキュリティ証明書の警告が表示されないことをご確認ください。

9.7.2 クライアント設定の初期化

ダイアログ内のチェックボックスには前回入力した値が記憶されている場合があります。これらの様々な設定をクライアント設定と読んでいますが、ユーザごとのクライアント設定は初期化することができます。

1. 画面右上のグローバルメニューにある、現在のログインユーザ名を押してください。
2. *クライアントの設定を元に戻す*ボタンを押し、続いて OK ボタンを押して終了してください。



10. 使用ポート一覧

netLD が通信に用いるポートを下に示します。デバイスにファイアウォールを通じてアクセスする必要がある場合には、 ファイアウォールの通信設定を変更し、必要なポートが解放されるようにしてください。

機能	プロトコル	ポート	UDP /TCP	通信方向
Zero-Touch	DHCP	67	UDP	netLD (←) 送信先
		68	UDP	netLD (→) 送信先
	HTTP	80	TCP	netLD (←) 送信先
	TFTP	69	UDP	netLD (←) 送信先
	ICMP	-	-	netLD (←) 送信先
自動ディスカバリ	SSH, Telnet	22,23	TCP	netLD (→) 送信先
	SNMP	161	UDP	netLD (→) 送信先
	ICMP	-	-	netLD (→) 送信先
設定の送信 (コンフィギュレーションの復元)	SSH, Telnet	22,23	TCP	netLD (→) 送信先
	TFTP	69	UDP	netLD (←) 送信先
	FTP	20,21	TCP	netLD (←) 送信先
変更ツールによる設定	SSH, Telnet	22,23	TCP	netLD (→) 送信先
Trap 送信	SNMP Trap	162	UDP	netLD (→) 送信先
リアルタイム変更検知	Syslog	514	UDP	netLD (←) 送信先
バックアップ*	SSH, Telnet	22, 23	TCP	netLD (→) 送信先
	SNMP	161	UDP	netLD (→) 送信先
	TFTP	69	UDP	netLD (←) 送信先
	FTP	20,21	TCP	netLD (←) 送信先
ターミナルプロキシ	SSH	2222	TCP	netLD (←) クライアント PC
	SSH, Telnet	22, 23	TCP	netLD (→) 送信先
Web ターミナル	HTTPS	443	TCP	netLD (←) クライアント (GUI)
	SSH, Telnet	22, 23	TCP	netLD (→) 送信先
クライアント	HTTPS	443	TCP	netLD (←) クライアント (GUI)
外部認証機能	LDAP	389	TCP	netLD (→) 認証サーバ
	RADIUS	1812	UDP	netLD (→) 認証サーバ

* 使用するプロトコルは適切な設定は、使うデバイスの種類によります。

例えば、

IOS デバイス　　：　CLI (Telnet, SSH)のみ、あるいは CLI と TFTP の両方。

Alaxala デバイス　：　CLI (Telnet, SSH), FTP あるいは SNMP。

11. デフォルトで存在するコンプライアンスルール

出荷時に同梱されているルールセットを以下に示します。

IOS インタフェース Auto-Duplex/Speed

インタフェース設定において、

- ■no ip address ：一致した場合、対象外
- ■shutdown command ：一致した場合、対象外
- ■duplex auto ：一致しなかった場合、違反
- ■speed auto ：一致しなかった場合、違反

IOS セキュア Enable Password

全体において、

- ■Service パスワード-encryption ：一致しなかった場合、違反
- ■enable secret ：一致しなかった場合、違反

IOS Telnet 接続制限

vty 設定の行において、

- ■access-class ~Access List~ ：一致しなかった場合、違反

IOS SSH のみ接続許可

vty 設定の行において、

- ■transport input ssh ：一致しなかった場合、違反
- ■transport input telnet ：一致した場合、違反

IOS 不要なサービスの無効化

以下のいずれかが一致した場合、違反

- ■no service tcp-small-servers
- ■no service udp-small-servers
- ■no ip bootp server
- ■no service finger
- ■no ip source-route
- ■no ip identd
- ■no ip http server

IOS セッションアイドルタイムアウト

vty 設定の行において、

- ■exec-timeout minutes ~timeout~ ：一致しなかった場合、違反

12. サポート OS/デバイス一覧

最新のサポートデバイス対応状況は、ロジックベインの Web サイトを参照してください。

https://www.lvi.co.jp/NetLD/pdf/adapter_list.pdf

13. クーロン

クーロンとは、ユーザの設定したスケジュールに基づいてコマンドなどを自動実行するプログラムです。netLD は、設定した日時にジョブを自動実行するため、cron4j を用いています。

この章の一部は cron4j ウェブサイトの抜粋及び翻訳です。（http://www.sauronsoftware.it/projects/cron4j/）

cron4j は Java プラットフォーム用のスケジューリングライブラリで、Unix 上の cron デーモンと同様に働きます。cron4j を用いると、Java アプリケーション上から、シンプルなルールに従って、どんなタスクでも正しい時間に実行することができます。

UNIX の crontab と同様のパターンを用いることができます。 パターンは 5 つのスペースで区切られた文字列です。それぞれの部分は以下の意味を持ちます。

分サブパターン。 一時間中のどの分に実行されるべきかを指定します。使用可能な数字は 0 から 59 です。

時間サブパターン。 一日中の何時に実行されるべきかを指定します。使用可能な数字は 0 から 24 です。

日付サブパターン。 一月中の何日に実行されるべきかを指定します。使用可能な数字は 0 から 31 ですが、特殊な文字 "L" を用いて、月の終わりを指し示すことができ ます。

月サブパターン。 一年の何月に実行されるべきかを指定します。使用可能な数字は 0 から 31 ですが、特殊な文字 "L" を用いて、月の終わりを指し示すことができ ます。値は 1 から 12 が有効ですが、略称として "jan", "feb", "mar", "apr", "may", "jun", "jul", "aug", "sep", "oct", "nov", "dec" を用いることもできます。

曜日サブパターン。 一週間の何曜日に実行されるべきかを指定します。使用可能な数字は 0(日曜日)から 6(土曜日)です。その他に、略称として"sun", "mon", "tue", "wed", "thu", "fri", "sat"も使えます。

スター・ワイルドカード*も用いることができます。これは、 例えば「毎分」、「毎時間」、 「毎日」、「毎月」、「毎週何曜日」という意味になります。 スケジューラは、5 つのサブパターンがすべて一致した時にタスクを実行します。

例：

5****

「xx 時 5 分」に実行する(00:05, 01:05, 02:05 など)

*****

「毎分」実行する

* 12 * * Mon

「月曜日 12 時台の毎分」実行する

59 11 * * 1,2,3,4,5

59 11 * * 1-5

「月、火、水、木、金曜日の 11:59AM」に実行する

13 クーロン

*/5 * * * *

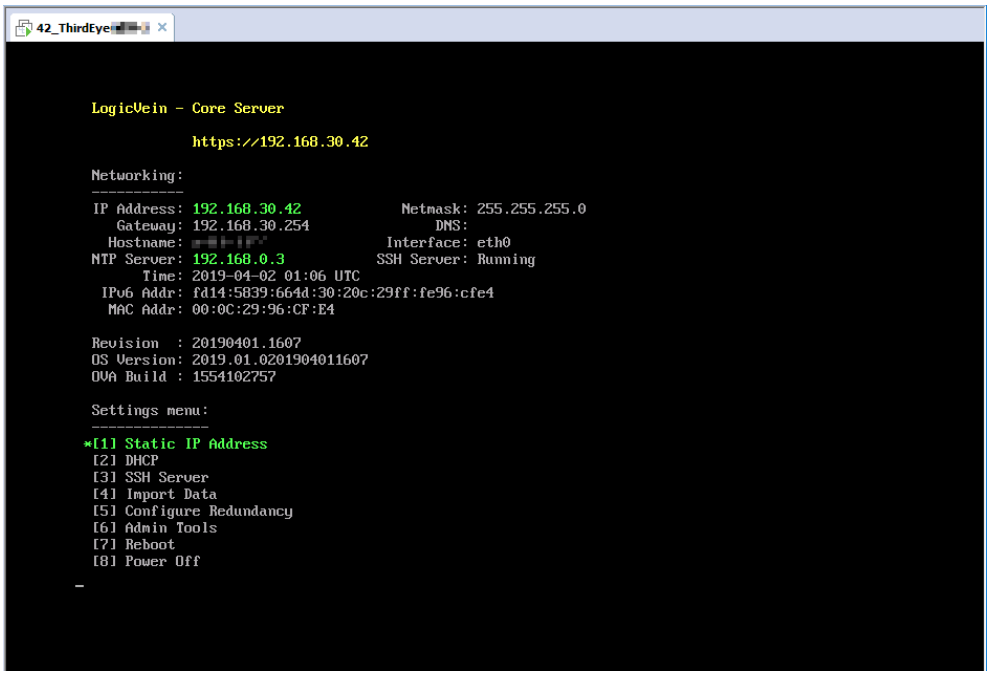
「5 分おき」に実行する(0:00, 0:05, 0:10, 0:15 など)

*/15 9-17 * * *

「9 時台~17 時台まで 15 分おき」に実行する(9:00, 9:15, 9:30…17:45)

14. 再起動／シャットダウン

再起動およびシャットダウンは、仮想マシンに接続して実行します。

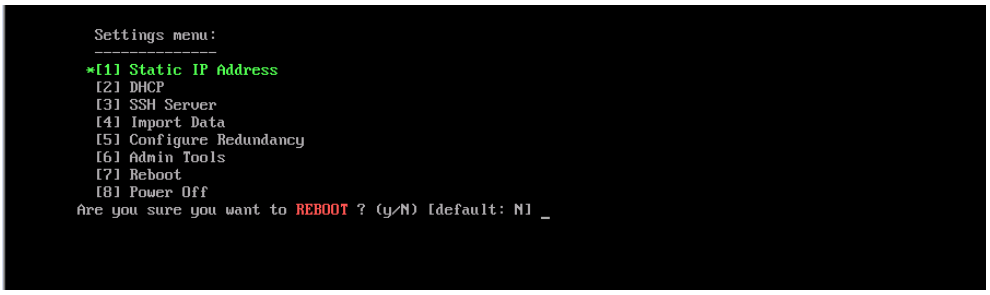


再起動する場合は、キーボードの「7」キーを押し［Reboot］を選択します。

シャットダウンする場合は、キーボードの「8」キーを押し［Power Off］を選択します。

メニュー選択後、確認メッセージが表示されるので、キーボードの「Y」キーを押し実行します。

【再起動】



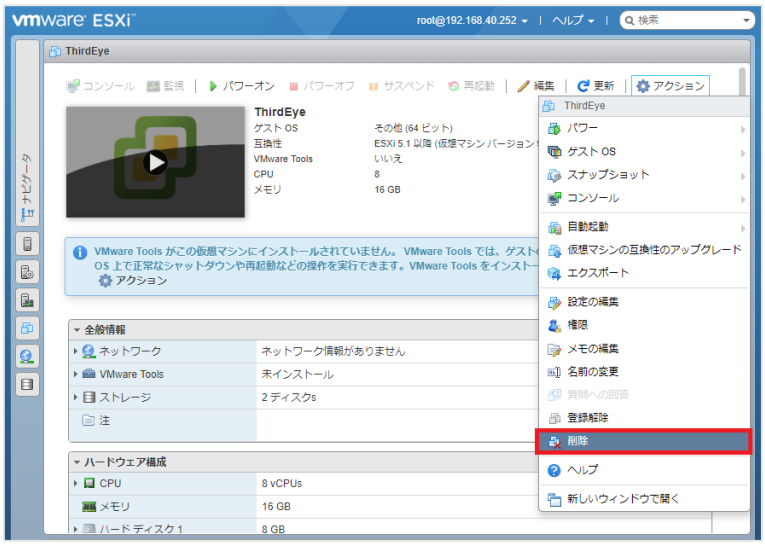
【シャットダウン】

15. アンインストール

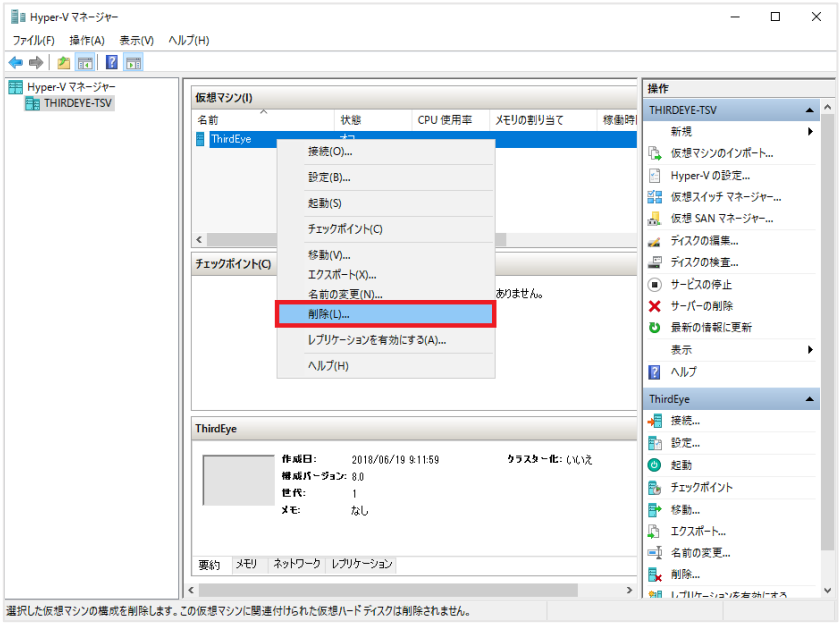
15.1 アンインストールする

1. netLD をシャットダウンします。
2. シャットダウン完了後、仮想のホスト OS から netLD の仮想マシンを削除します。

- VMware ESXi 6.5 での削除画面（例）



- Windows Hyper-V での削除画面（例）



以上で netLD のアンインストールは完了です。

16. お問い合わせ

netLD の操作中に問題や疑問が生じた場合は、下記の弊社サポートまでお問い合わせください。

お問い合わせの前に、あらかじめ下記の必要事項をご確認ください。

【必須事項】

① 製品名

② 製品のバージョン情報（リビジョンを含む）

③ 製品のシリアル番号（netLD のライセンス情報）

④ 具体的な症状や疑問点

※ スクリーンショットをお送りいただけると、情報共有を円滑に行うことができ、問題の解決に役立つことがあります。

■お問い合わせ先■

株式会社ロジックベイン　サポート窓口

電話：　044-871-4010

メール：　support@lvi.co.jp

受付時間：平日 9:00～12:00／13:00～17:00 （※土・日・祝日および弊社休業日を除く）