東陽テクニカ
SYNESIS
管理者マニュアル

2020/2/28

A010-1799-95 Rev.C

改訂履歴

版数	改訂日	内容
Rev.A	2017/12/22	初版
Rev.B	2018/11/05	v4.0
Rev.C	2020/2/26	V5.0(html 化)

著作権・商標

このマニュアルのいかなる部分も株式会社東陽テクニカの書面による許可なしに、形態、方法を問わず、複写、送信、転載、検索システムへの保存、及び他言語に翻訳することを禁じます。

SYNESIS および PacketReplayer(パケットリプレイヤー)は、株式会社東陽テクニカの登録商標または商標です。
Microsoft は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
Windows の正式名称は、Microsoft Windows Operating System です。
Linux は、Linus Torvalds 氏の米国およびその他の国における登録商標または商標です。
Ubuntu は、Canonical Ltd.の商標または登録商標です。
Intel、Pentium、Xeon、Celeron は、Intel Corporation またはその子会社の米国およびその他の国における登録商標または商標です。
Java およびすべての Java 関連の商標は、米国 Oracle Corporation の米国およびその他の国における登録商標または商標です。
Apache、Tomcat は、Apache Software Foundation の登録商標または商標です。
Ethernet は、米国 XEROX Corporation の登録商標です。
DELL、PowerEdge は、Dell Inc.の米国およびその他の国における登録商標または商標です。
本文中のその他の登録商標及び商標はそれぞれの所有者に帰属します。
本文中、®（登録商標）、© （コピーライト） 等の各商標マークは省略しています。

目次

改訂履歴 i
著作権・商標 ii
1. 本書について 4
1.1. 表記規則および略号 4
1.2. SYNESIS の種類 4
1.2.1. ラックマウント (1U) 4
1.2.2. ラックマウント (2U) 5
1.2.3. ラックマウント (2U) ストレージ・ユニット有 5
1.2.4. ポータブル 5
2. SYNESIS の起動・停止・再起動 6
2.1. 起動 6
2.1.1. SYNESIS Distributed の場合 6
2.1.2. SYNESIS Portable の場合 6
2.2. 停止 7
2.2.1. 共通手順 7
2.2.2. SYNESIS Distributed の場合 8
2.3. OS の再起動 9
2.3.1. GUI (デスクトップ)から実施する場合 9
2.3.2. SSH または Terminal から実施する場合 9
2.4. SYNESIS サービスの再起動 10
2.4.1. 各サービスの役割と再起動時のキャプチャ停止の有無 10
3. SYNESIS へのアクセス方法 11
3.1. アクセス方法一覧(開放ポート) 11
3.2. Ubuntu OS 12
3.2.1. リモートデスクトップ 12
3.2.2. SSH 13
3.3. SYNESIS ソフトウェア 14
3.3.1. メイン GUI 14
3.3.2. サービス・ログ管理 GUI 14
3.4. iDRAC 15
3.4.1. iDRAC8 (Integrated Dell Remote Access Controller 8) 15

3.4.2. iDRAC9 (Integrated Dell Remote Access Controller 9) 16
4. 初期設定の変更 17
4.1. Ubuntu OS の初期設定変更 17
4.1.1. ホスト名 17
4.1.2. 管理者アカウント(ユーザ名・パスワード) 18
4.1.3. 管理ポートのネットワーク設定 19
4.2. SYNESIS の初期設定変更 20
4.2.1. Firewall 設定 20
4.2.2. サーバ証明書の変更 22
4.2.3. NTP サーバ 23
4.2.4. SMTP サーバ 25
4.3. iDRAC の初期設定変更 26
4.3.1. iDRAC ポートのネットワーク設定 26
4.3.2. SMTP サーバの設定 30
5. アカウント管理 32
5.1. Ubuntu OS のアカウント 32
5.1.1. Ubuntu OS のアカウント作成 32
5.1.2. Ubuntu OS のアカウント変更 33
5.1.3. Ubuntu OS のアカウント削除 34
5.2. SYNESIS のアカウント 35
5.2.1. メイン GUI 35
5.2.2. サービス・ログ管理 GUI 37
5.3. iDRAC のアカウント 38
5.3.1. iDRAC8 38
5.3.2. iDRAC9 42
6. SYNESIS の監視機能 44
6.1. iDRAC：ハードウェアの監視 44
6.1.1. iDRAC8 44
6.1.2. iDRAC9 48
6.2. SYNESIS ソフトウェア：キャプチャ動作中の異常監視 52
6.2.1. 通知先、通知手段の設定 52
6.2.2. 通知するイベントの設定 55
6.3. SYNESIS ソフトウェア：キャプチャトラフィックの状態監視 56
6.3.1. アラートの設定 57

7. 設定情報やデータのバックアップ 59
7.1. OS 設定情報のバックアップ 59
7.2. SYNESIS 環境・設定情報 60
7.2.1. ライセンス・ファイルのバックアップ 60
7.2.2. コンフィグ・ファイルのバックアップ 60
7.3. キャプチャ・データのバックアップ 62
7.4. トレースファイルのバックアップ 63
7.5. 作成されたレポートのバックアップ 64
8. 設定情報やデータのリストア 65
8.1. OS 設定情報のリストア 65
8.2. SYNESIS 環境・設定情報のリストア 66
8.2.1. ライセンス・ファイルのリストア 66
8.2.2. コンフィグ・ファイルのリストア 67
8.3. トレース・ファイルのリストア 71
8.4. レポート設定のリストア 71
9. 簡易動作確認手順 72
9.1. キャプチャポートのリンクステータス確認 72
9.2. SYNESIS へのアクセス 72
9.3. キャプチャの動作確認 73
9.3.1. SYNESIS の設定の確認 73
9.3.2. キャプチャの開始 74
9.3.3. キャプチャ開始後の確認項目 74
9.4. iDRAC のステータス確認 75
9.4.1. iDRAC8 75
9.4.2. iDRAC9 76
10. 障害・異常発生時の対応手順 77
10.1. 発生した事象のまとめ 77
10.2. 簡易動作確認の実施と結果の確認 77
10.3. ログの取得 78
10.4. お問い合わせ 78
11. ログの取得 79

1.本書について

本書は、SYNESIS の管理者向けマニュアルです。

モデルによって運用・管理に必要な各種設定や操作方法が異なりますので、ご利用前にお使いのモデルを確認してください。

SYNESIS のモデルについての詳細は「1.2.SYNESIS の種類」をご参照ください。

なお、本書に示される画面は開発中のものです。画面デザインおよび画面に表示されている文言が、ご利用の製品に表示される画面と若干異なる場合があります。

本書に示される画面は開発中のものです。画面デザインおよび画面に表示されている文言が、ご利用の製品に表示される画面と若干異なる場合があります。

操作に不明な点が生じた場合には、ユーザーガイドをご参照いただくか、弊社お問い合わせ先までお問い合わせください。

1.1. 表記規則および略号

本書で使用する表記規則は下記の通りです。

項番	表記	使用目的
1	□	半角スペースを意味します。
2	〈*任意の文字*〉	変数を意味します。動作環境に合わせて適宜設定します。
3	`Command`	コマンド入力例を意味します。
4	[メニュー名]	操作画面上に表示されるメニューや設定項目を意味します。
5	<ボタン>	操作画面上に表示されるボタンを意味します。

なお、記号は特に断りがない限り、原則半角で表現します。

1.2. SYNESIS の種類

SYNESIS にはラックマウント・タイプとポータブル・タイプがあります。

モデルによって作業手順が異なる部分もありますので、写真を参考に、ご使用の SYNESIS の種類をご確認ください。

1.2.1. ラックマウント (1U)

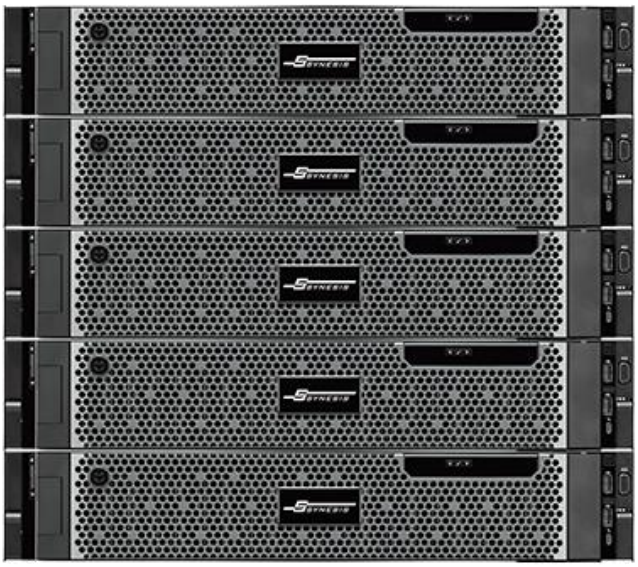
１Ｕタイプのラックマウントです。

1.2.2. ラックマウント (2U)

２Ｕタイプのラックマウントです。本体（コントローラ・ユニット）のみになります。

1.2.3. ラックマウント (2U) ストレージ・ユニット有

コントローラ・ユニットと１台以上のストレージ・ユニットのセットになります。



1.2.4. ポータブル

持ち運び可能なポータブル・タイプです。

2.SYNESIS の起動・停止・再起動

本章では、SYNESIS の起動・停止・再起動手順について説明いたします。手順は、モデルによって異なりますので、ご利用のモデルに該当する手順を実施してください。

2.1. 起動

2.1.1. SYNESIS Distributed の場合

2.1.1.1. ストレージ・ユニットの電源 On

1) ストレージ・ユニット(MD1420/MD1200)がある場合は、背面の電源スイッチ 2 つを電源 On にします。※MD1420/MD1200 が複数ある場合、これらのどれから電源を On にしても構いません。

MD1420

MD1200

2) ストレージ・ユニット(MD1420/MD1200)前面にある、HDD の緑色 LED の点滅が終わる(点灯状態になる)まで待ちます。

3) ストレージ・ユニット(MD3400)がある場合は、背面の電源スイッチ 2 つを電源 On にします。

MD3400

4) ストレージ・ユニット(MD3400)前面にある、HDD の緑色 LED の点滅が終わる(点灯状態になる)まで待つ、または、MD1420/MD1200 の LED と共に点滅することを確認します。

2.1.1.2. コントローラ・ユニットの電源 On

ストレージ・ユニットがある場合、それらの電源 On が完了していることを確認します。

コントローラ・ユニット前面にある、電源ボタンを押します。

2.1.2. SYNESIS Portable の場合

SYNESIS Portable の電源ボタンを押し、電源を ON にします。

2.2. 停止

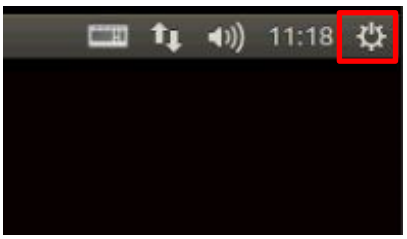
2.2.1. 共通手順

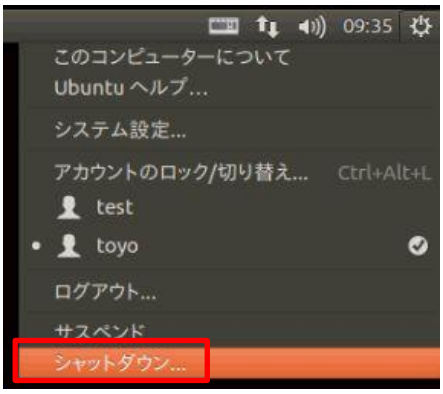
ご利用のモデルにかかわらず、以下の手順を実施します。その後ご利用のモデルに該当する手順を実施してください。

2.2.1.1. GUI(デスクトップ)から実施する場合

KVM 接続時のみ実施できます。リモート実施は「2.2.1.2 SSH または Terminal から実施する場合」から実施してください。

1) デスクトップ画面右上のボタンをクリックし、[**シャットダウン**] をクリックします。





2) ダイアログが表示されるので [**シャットダウン**] をクリックします。

3) HDD の LED が消灯するまで待ちます。

4) ストレージユニットのある SYNESIS Distributed をご使用の場合、続いて「2.2.2.1 ストレージ・ユニットの電源 Off」の記述に従ってください。

2.2.1.2. SSH または Terminal から実施する場合

1) PuTTY などのターミナルエミュレータを利用して、SYNESIS に SSH で接続します。

接続先　：SYNESIS 管理ポートの IP アドレス

ユーザ 名（※デフォルト）：synesis

パスワード(※デフォルト)：admin

2) 以下のコマンドを入力し、コントローラをシャットダウン(電源 Off)します。

コマンド：`sudo□shutdown□-h□now`

3) コントローラ・ユニットの HDD の LED が消灯するまで待ちます。

4) ストレージユニットのある SYNESIS Distributed をご使用の場合、続いて「2.2.2.1 ストレージ・ユニットの電源 Off」の記述に従ってください

2.2.2. SYNESIS Distributed の場合

2.2.2.1. ストレージ・ユニットの電源 Off

1) ストレージ・ユニット(MD1420/MD1200)がある場合は、「2.2.1.1 GUI(デスクトップ)から実施する場合」または「2.2.1.2 SSH または Terminal から実施する場合」が完了していることを確認し、MD1420/1200 背面の電源スイッチを Off にします。

※MD1420/MD1200 が複数ある場合、これらのどれから電源を Off にしても構いません。

MD1420

MD1200

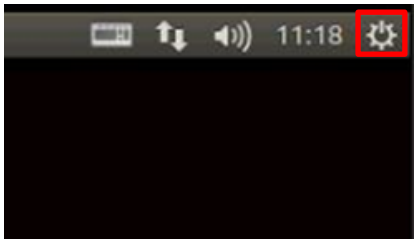
2) ストレージ・ユニット(MD3400)がある場合は、コントローラ・ユニットの電源が Off になっていることを確認し、MD3400 背面の電源スイッチを Off にします。

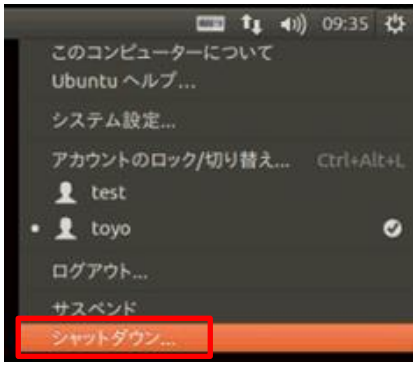
MD3400

2.3. OS の再起動

2.3.1. GUI (デスクトップ)から実施する場合

1) デスクトップ画面右上のボタンをクリックし、[**シャットダウン**] をクリックします。





2) ダイアログが表示されるので [**再起動**] をクリックします。

2.3.2. SSH または Terminal から実施する場合

1) PuTTY などのターミナルエミュレータを利用して、SYNESIS に SSH で接続します。

接続先　：SYNESIS 管理ポートの IP アドレス

ユーザ 名（※デフォルト）：synesis

パスワード(※デフォルト)：admin

Terminal で実施する場合は、SYNESIS の OS 上で Terminal を起動します。

2) 以下のコマンドを入力し、OS を再起動します。

コマンド：`sudo□reboot`

または、

コマンド：`sudo□shutdown□-r□now`

2.4. SYNESIS サービスの再起動

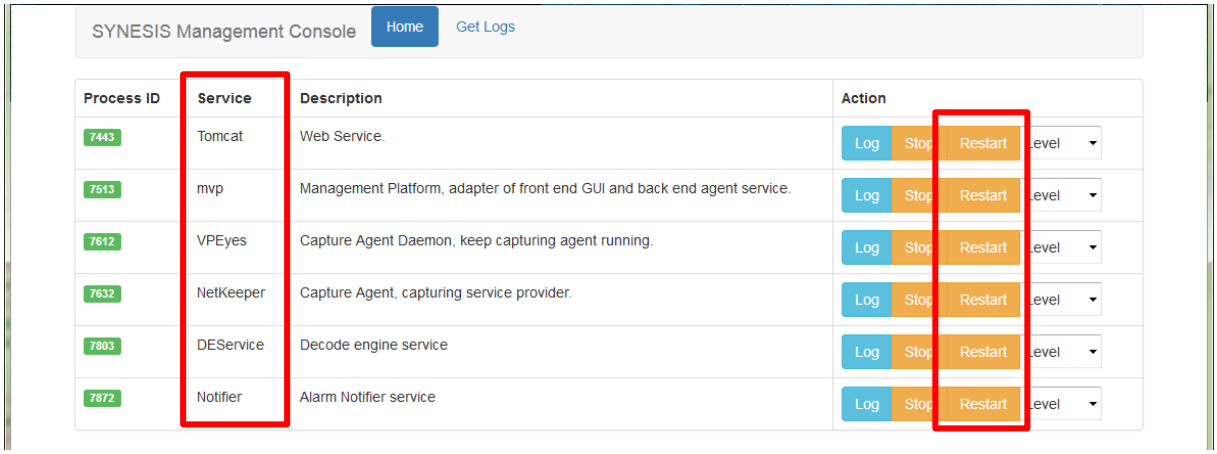
SYNESIS の各種サービスをサービス・ログ管理画面から再起動することができます。

サービスによっては、再起動時にキャプチャが停止しますので、ご注意ください。 (詳細は「2.4.1. 各サービスの役割と再起動時のキャプチャ停止の有無」をご参照ください。)

SYNESIS サービスの再起動手順は以下の通りです。

1) SYNESIS のサービス・ログ管理 GUI へアクセスします。 ※「3.3.2.1 ログイン」参照

2) 以下の画面が表示されるので、再起動したいサービスの"Restart"ボタンをクリックします。



3) クリックしたボタンの色が薄い間はサービスの再起動中です。色が元に戻れば再起動は完了です。

2.4.1. 各サービスの役割と再起動時のキャプチャ停止の有無

各サービスの役割は以下の通りです。

サービス名	役割	キャプチャの停止
Tomcat	WEB UI	なし
mvp	各プロセスへの API の提供	なし
NetKeeper	キャプチャ，解析	あり(停止する)
VPEyes	NetKeeper の死活監視(NetKeeper と連動)	
DEService	リアルタイムデコード	なし
Notifier	メールや SNMPTrap などによる通知	なし

NetKeeper を再起動すると実行中のキャプチャは停止します。 再起動後、自動的にキャプチャが再開されるよう、設定することが可能です。

詳細はユーザーガイドの「3-3-1-2-1. 共通オプション」をご参照ください。

3.SYNESIS へのアクセス方法

本章では、SYNESIS を運用・管理するのに必要なアクセス方法を説明します。

SYNESIS を構成する主なソフトウェアは以下の通りです。

ソフトウェア		主な役割
OS (Ubuntu OS)		OS
SYNESIS ソフトウェア	メイン GUI	パケットキャプチャとその分析、操作 GUI
	サービス・ログ管理 GUI	SYNESIS サービスの操作、ログの確認・収集
iDRAC		ハードウェアのステータスを監視・通知 ※SYNESIS Portable を除く

詳しい手順については、各リンク先をご参照ください。

3.1. アクセス方法一覧(開放ポート)

SYNESIS を構成するソフトウェアへのアクセス方法は下記の通りです。

アクセス先		プロトコル	開放ポート	IP アドレス(デフォルト) 物理ポート：アドレス	管理者権限アカウント(デフォルト)
OS (Ubuntu OS)		RDP	TCP:3389	eno1: 172.22.201.250 eno2-eno4： DHCP	synesis/admin
		SSH	TCP:22		
SYNESIS ソフトウェア	メイン GUI	HTTPS	TCP:443		admin/synesis1
	サービス・ログ管理 GUI				
iDRAC		HTTPS	TCP:443	iDRAC: 192.168.0.120	root/calvin

具体的な詳しい手順は、それぞれのリンク先をご参照ください。

3.2. Ubuntu OS

3.2.1. リモートデスクトップ

Windows のリモートデスクトップ機能で Ubuntu OS にログインすることができます。

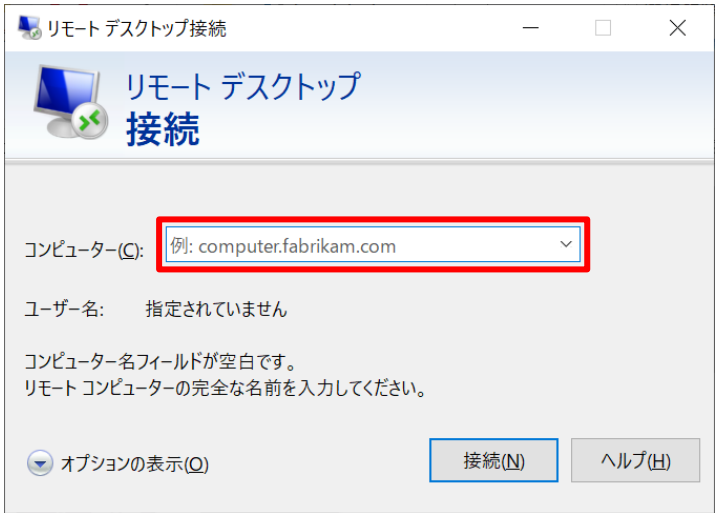
※接続は 1 セッションのみです。

3.2.1.1. ログイン

1) Windows のスタートボタンをクリックし、[**すべてのプログラム**] をクリックします。

2) [**アクセサリ**] をクリックし、メニューを展開します。

3) [**リモートデスクトップ接続**] をクリックしてください。以下の画面が表示されます。

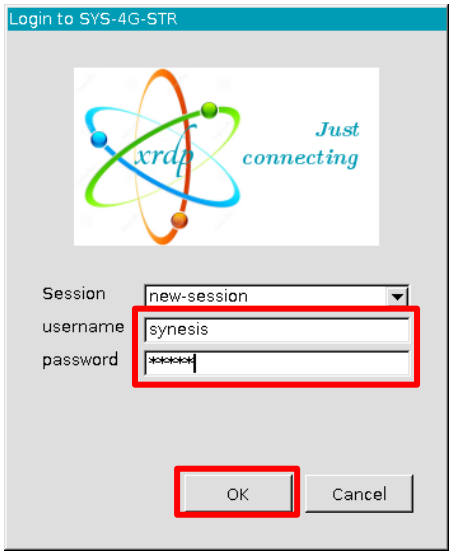


4) [**コンピュータ(C)**]の欄に SYNESIS の管理ポートの IP アドレスを入力して、<**接続**> をクリックしてください。

信頼や接続の確認画面が表示された場合は「接続」もしくは「はい」をクリックし接続します。

5) 接続に成功すると、下記のログイン画面が表示されます。

[**Session**] 欄は "new-session" を選択し、OS のユーザ名とパスワードを [**username**] 欄、[**password**] 欄それぞれに入力後してください。



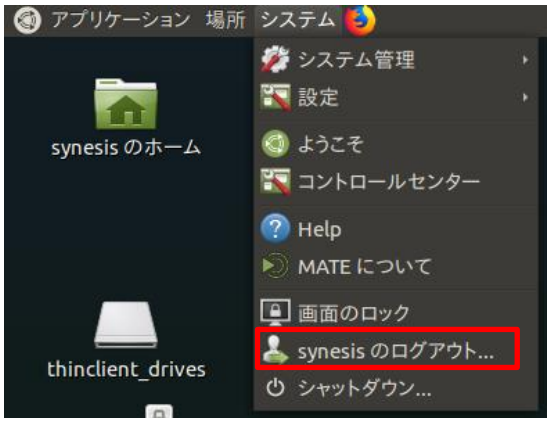
6) 入力後、<**OK**> をクリックします。

7)　ログインに成功すると、OS のデスクトップ画面が表示されます。

3.2.1.2. ログアウト

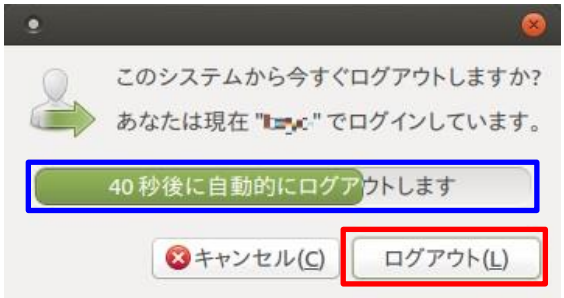
1)　画面左上部の [**システム**] をクリックし、メニューを表示させます。

メニューから [**XXXXのログアウト…**] をクリックします。



2)　確認ダイアログで [**ログアウト**] をクリックします。

※自動ログアウトのカウントダウン(青枠)もされており、表示されている時間が経過すれば何もしなくても自動でログアウトされます。



3.2.2.　　SSH

SSH クライアント接続で Ubuntu OS にログインすることができます。

3.2.2.1. ログイン

1)　SSH クライアントにて SYNESIS 管理ポートの IP アドレスへアクセスします。

2)　ユーザ名・パスワードを入力しログインします。

3.2.2.2. ログアウト

コマンドライン上で「***exit***」コマンドを入力し、ログアウトします。

3.3. SYNESIS ソフトウェア

SYNESIS には Web ブラウザを用いてアクセスします。

3.3.1. メイン GUI

3.3.1.1. サインイン

1) 下記のアドレスを Web ブラウザのアドレスバーに入力すると、SYNESIS にアクセスできます。

https://〈*管理ポートの IP アドレス*〉/

2) 以下の画面が表示されるので、SYNESIS アカウントのユーザ名、パスワードを入力して、「サインイン」ボタンをクリックします。

3.3.1.2. サインアウト

ツールバー右上の**<サインアウト>**ボタン をクリックします。

サインアウトを行うと、サインイン画面に戻ります。

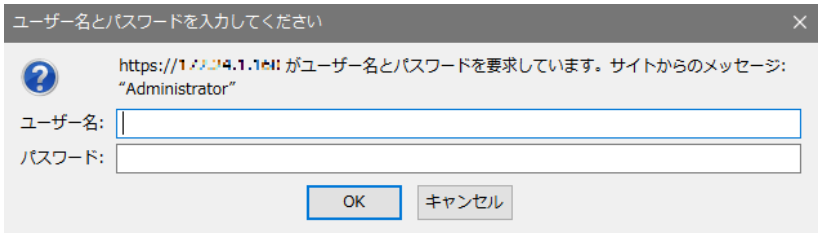
3.3.2. サービス・ログ管理 GUI

3.3.2.1. ログイン

1) 下記のアドレスを Web ブラウザのアドレスバーに入力します。

https://〈*管理ポートの IP アドレス*〉/mgmt/

2) 以下の画面が表示されるので、SYNESIS サービス・ログ管理 GUI 用アカウントのユーザ名、パスワードを入力して、 <**OK**>ボタンをクリックしてください。



3.3.2.2. ログアウト

ブラウザの本ページを閉じます。

3.4. iDRAC

SYNESIS Distributed をご利用の場合、iDRAC (integrated Dell Remote Access Controller)でサーバのリモート管理を行うことができます。SYNESIS Portable では本機能をご利用いただけません。

ご利用のモデルによって iDRAC のタイプが異なります。タイプはログイン画面等に表示されている iDRAC 名称(Integrated Dell Remote Access Controller)に続く数字を確認してください。最後の数字が「8」の場合は「iDRAC8」、「9」の場合は「iDARC9」になります。

以降、iDRAC に関する記述を参照する際は該当するタイプの記述を参照してください。

なお、iDRAC には Web ブラウザを用いてアクセスします。

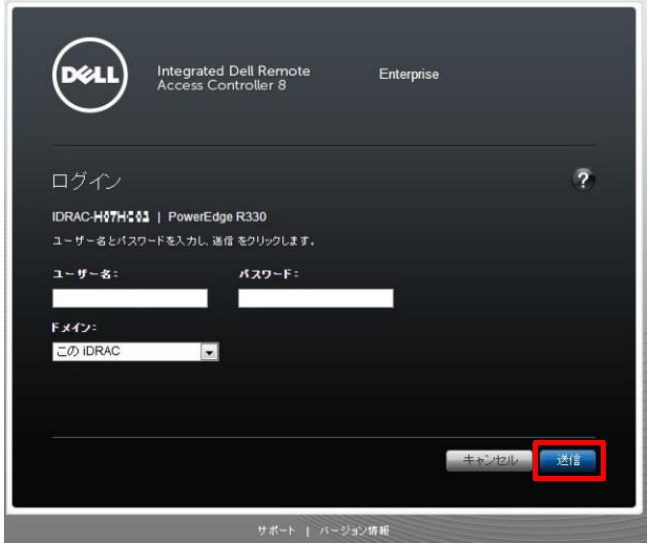
3.4.1. iDRAC8 (Integrated Dell Remote Access Controller 8)

3.4.1.1. ログイン

1) 下記のアドレスを Web ブラウザのアドレスバーに入力すると、iDRAC にアクセスできます。

https://〈*iDRAC ポートの IP アドレス*〉/

2) 以下のようなログイン画面が表示されます。



※[Integrated Dell Remote Access Controller 8] の最後の数字が「8」であることを確認してください。最後の数字が「9」の場合は、「iDARC9」の手順を参照してください。

3) ユーザー名・パスワードを入力し<送信>ボタンをクリックしてください。

3.4.1.2. ログアウト

画面右上の [**ログアウト**] をクリックしログアウトします。

3.4.2. iDRAC9 (Integrated Dell Remote Access Controller 9)

3.4.2.1. ログイン

1) 下記のアドレスを Web ブラウザのアドレスバーに入力すると、iDRAC にアクセスできます。

https://〈*iDRAC ポートの IP アドレス*〉/

2) 以下ようなのログイン画面が表示されます。

※[Integrated Remote Access Controller 9] の最後の数字が「9」であることを確認してください。最後の数字が「8」の場合は、「iDRAC8」の手順を参照してください。

3) ユーザー名、パスワードを入力し<**ログイン**>ボタンをクリックしてください。

3.4.2.2. ログアウト

1) 画面右上の をクリック後 [**ログアウト**] をクリックします。

4.初期設定の変更

本章では、SYNESIS を構成する各ソフトウェアのアカウントやネットワーク設定などを、 必要に合わせて初期設定から変更するための手順を解説します。

4.1. Ubuntu OS の初期設定変更

4.1.1. ホスト名

ホスト名を変更する場合は、以下の手順を実施します。

なお、ホスト名に関する制限は以下の通りです。

項目	制限
ホスト名文字数	最大 15 文字
ホスト名文字列	アルファベット(A-Z, a-z) 数字(0-9) ハイフン(-) 先頭文字はアルファベット、末尾はハイフン以外

1) SYNESIS のローカルから Terminal を起動するか、リモートから SSH で接続します。

※「3.2.2 SSH」参照

2) 以下の 2 つのコマンドを入力します。

```
コマンド：sudo□sed□-i□-e□'1s/.*/<新ホスト名を入力>/g'□/etc/hostname
コマンド：sudo□sed□-i□-e□'/127.0.1.1/□c□127.0.1.1¥t<新ホスト名を入力>'□/etc/hosts
```

3) 以下の 2 つのコマンドを入力し、出力結果を確認します。

```
コマンド：cat□/etc/hostname
        :〈変更したホスト名〉                (←出力)
コマンド：cat□/etc/hosts
        : 127.0.0.1   localhost             (←出力)
        : 127.0.1.1 〈変更したホスト名〉     (←出力)
```

4) OS を再起動してください。 ※「2.3 OS の再起動」参照

4.1.2. 管理者アカウント(ユーザ名・パスワード)

ユーザ名の変更には、変更したいアカウント以外で管理者権限を持つアカウントが必要になります。初期設定では、管理者権限を持つアカウントは 1 つしかないため、一時的なアカウントを作成してから変更を行います。以下の手順を順番に行ってください。

1) SYNESIS のローカルから Terminal を起動するか、リモートから SSH で接続します。
   ※「3.2.2 SSH」参照

2) 下記コマンドを入力し、管理者権限を持つ一時的なアカウントを作成します。
   ※詳細は、「5.1.1 Ubuntu OS のアカウント作成」を参照してください。

```
〈ﾛｸﾞｲﾝﾕｰｻﾞ名〉@〈ﾎｽﾄ名〉:~$ sudo□adduser□〈一時ｱｶｳﾝﾄのﾕｰｻﾞ名〉
〈ﾛｸﾞｲﾝﾕｰｻﾞ名〉@〈ﾎｽﾄ名〉:~$ sudo□usermod□-G□sudo□〈一時ｱｶｳﾝﾄのﾕｰｻﾞ名〉
```

3) OS を再起動します。　※「2.3 OS の再起動」参照

4) 「5.1.2.1 ユーザ名の変更」の手順に従い、ユーザ名とパスワードを変更します。

5) 変更後の管理者アカウントでログイン後、下記コマンドを入力し、管理者権限を持つ一時的なアカウントを削除します。

```
〈ﾛｸﾞｲﾝﾕｰｻﾞ名〉@〈ﾎｽﾄ名〉:~$ sudo□userdel□-r□〈一時ｱｶｳﾝﾄのﾕｰｻﾞ名〉
```

4.1.3. 管理ポートのネットワーク設定

1) SYNESIS のローカルから Terminal を起動するか、リモートから SSH で接続します。

※「3.2.2 SSH」参照

2) エディタ(vi)で interface ファイルをオープンします。以下のコマンドを入力してください。

コマンド：sudo□vi□/etc/network/interfaces

3) 以下の記述が表示されますので、[i]キーを押して挿入(INSERT)モードに移行します。

```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

auto eno1                          #固定 IP を設定したい管理ポートを記載
iface eno1 inet static             #固定 IP を設定したい管理ポートを記載
address 172.22.201.250             #対象の管理ポートに設定したい内容を記載
gateway 172.22.254.254             #同上
netmask 255.255.0.0                #同上
network 172.22.0.0                 #同上
broadcast 172.22.255.255           #同上
dns-nameservers 172.22.254.254     #設定不要な場合は#にてコメントアウト
-----------------------------------------------------------------------------------------
例：他のポート(eno2-eno4)も固定 IP アドレスにする場合
auto eno2
iface eno2 inet static
address 172.22.201.251
…
…
…
```

4) 固定の IP アドレスを設定する場合は、管理ポートごとに上図の赤字部分と同様の記述を追記(変更)してください。

DHCP に設定する場合は、上図赤字と同様の記述箇所を#でコメントアウトするか、削除します。

5) 設定を変更しましたら、[Esc]キーを押し、その後「:x」と入力して[Enter]キーを押します。

変更が保存され、エディタが終了します。

6) OS を再起動します。 ※「2.3 OS の再起動」参照

4.2. SYNESIS の初期設定変更

SYNESIS の使用を開始する前に、ご利用の環境に合わせて SYNESIS の設定を変更してください。

4.2.1. Firewall 設定

SYNESIS で利用していないポートは、SYNESIS 上の Firewall にて通信が遮断されています。SNMP トラップトリガ機能を利用する場合などは、使用するポートの通信を許可してください。また、通信が不要になったポートは、通信遮断の設定を行ってください。

4.2.1.1. Firewall の設定の確認

以下のコマンドで、現在の Firewall の設定を確認できます。

コマンド：`sudo□ufw□status□verbose`

※表示例

```
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
To                  Action          From
--                  ------          ----
22                  ALLOW IN        Anywhere
80                  ALLOW IN        Anywhere
443                 ALLOW IN        Anywhere
3389                ALLOW IN        Anywhere
22 (v6)             ALLOW IN        Anywhere (v6)
80 (v6)             ALLOW IN        Anywhere (v6)
443 (v6)            ALLOW IN        Anywhere (v6)
3389 (v6)           ALLOW IN        Anywhere (v6)
```

4.2.1.2. 指定ポートの通信許可

特定ポートの通信を許可するには、以下の手順を実行してください。

1) 以下のコマンドを実行します。

コマンド：`sudo□ufw□allow□<許可したいポート番号>`

2) 「4.2.1.1.Firewall の設定の確認」の手順に従い、手順 1)で指定したポートが追加されていることを確認します。

3) 以下のコマンドを実行します。

コマンド：`sudo□systemctl□restart□ufw`

4.2.1.3. 指定ポートの通信遮断

通信が許可されているポートの通信を遮断するには、以下の手順を実施してください。

※本手順は、「4.2.1.2.指定ポートの通信許可」で通信を許可したポートにのみ適用可能です。

1) 以下のコマンドを実行します。

コマンド：`sudo□ufw□status□numbered`

2) 以下のような結果が得られますので、通信を遮断したいポートの最左列の番号を控えておきます。

※以降の記述は、ポート番号 162 を遮断する場合の例です。

```
     To                         Action      From
     --                         ------      ----
[ 1] 22                         ALLOW IN    Anywhere
[ 2] 80                         ALLOW IN    Anywhere
[ 3] 443                        ALLOW IN    Anywhere
[ 4] 3389                       ALLOW IN    Anywhere
[ 5] 162                        ALLOW IN    Anywhere
[ 6] 22 (v6)                    ALLOW IN    Anywhere (v6)
[ 7] 80 (v6)                    ALLOW IN    Anywhere (v6)
[ 8] 443 (v6)                   ALLOW IN    Anywhere (v6)
[ 9] 3389 (v6)                  ALLOW IN    Anywhere (v6)
[10] 162 (v6)                   ALLOW IN    Anywhere (v6)
```

3) 手順 2)で控えた番号の内、大きい数値から順番に以下のコマンドを繰り返します。

コマンド：`sudo□ufw□delete□<遮断したいポートの最左列に記載の番号>`

```
例)
$sudo ufw delete 10
Deleting:
allow 162 (v6)
Proceed with operation (y|n)? y <-間違いがなければ"y"を入力
Rule deleted
$sudo ufw delete 5
Deleting:
allow 162
Proceed with operation (y|n)? y <-間違いがなければ"y"を入力
Rule deleted
```

4) 4.2.1.1 章に従い、手順 3)で指定したポートが削除されていることを確認します。

5) 以下のコマンドを実行します。

コマンド：`sudo□systemctl□restart□ufw`

4.2.2. サーバ証明書の変更

SYNESIS ではバージョン v4.0 より、SSL/TLS 通信を標準にしております。SSL/TLS 通信に用いる証明書を出荷時に添付しておりますが、お客様のご用意した証明書に変更することが可能です。

証明書を変更する場合は、以下の手順を実施してください。変更しない場合は、本手順は不要です。

➢ 注意事項

- CA 証明書、サーバ証明書、及び、サーバ証明書の鍵ファイルの 3 つをご用意下さい。
- 証明書の作成手順については環境により複数の方法があるため、必要な場合はお客様のシステム、又は、ネットワーク管理者へお問い合わせください。
- 証明書と鍵ファイルは PEM 形式(拡張子:.pem)、又は、DER 形式(拡張子:.cer,.der)である必要があります。

1) 用意した証明書と証明書の鍵ファイルを "/etc/nginx/synesis" にコピーします。

※例として、以下のファイルを用意したものとして手順を記載します

- CA 証明書: dummy_ca.pem
- サーバ証明書: dummy_server.pem
- サーバ証明書の鍵: dummy_serverkey.pem

2) vi 等のテキストエディタで "/etc/nginx/synesis/synesis.conf" を開き、以下の変更を行います。

- "ssl_catificate"の右側のパスをサーバ証明書のパスに修正する
- "ssl_catificate_key"の右側のパスをサーバ証明書の鍵ファイルのパスに修正する
- "ssl_trusted_catificate"の右側のパスを CA 証明書のパスに修正する

```
〈ログインユーザ名〉@〈ホスト名〉:~$ sudo□su□-
[sudo] password for 〈ログインユーザ名〉: パスワードを入力
〈ログインユーザ名〉@〈ホスト名〉:~# vi□/etc/nginx/synesis/synesis.conf
# Settings for Synesis

# SSL/TLS Settings
ssl_certificate          /etc/nginx/synesis/dummy_server.pem;     ← サーバ証明書のパスに修正する
ssl_certificate_key      /etc/nginx/synesis/dummy_serverkey.pem;  ←サーバ証明書の鍵ファイルのパスに修正する
ssl_trusted_certificate  /etc/nginx/synesis/dummy_ca.pem;         ← CA 証明書のパスに修正する
ssl_dhparam              /etc/nginx/synesis/dhparam.pem;
…
```

3) 保存して、テキストエディタを閉じます。※vi の場合 ":wq" を入力する。

4) 以下のコマンドを入力し、エラーが無いことを確認します。

コマンド：`sudo□nginx□-t`

5) 以下のコマンドを入力して、設定の再読み込みを行います。

コマンド：`sudo□nginx□-s□reload`

6) 以下のコマンドを入力し、Java のキーストアに証明書を登録します。

コマンド：`sudo□keytool□-import□-file□/etc/nginx/synesis/dummy_server.pem □-keystore□/etc/ssl/certs/java/cacerts`

※パスワード：changeit

7) 以下のコマンドを入力し、Tomcat の再起動を行います。

コマンド：`sudo□service□tomcat7□restart`

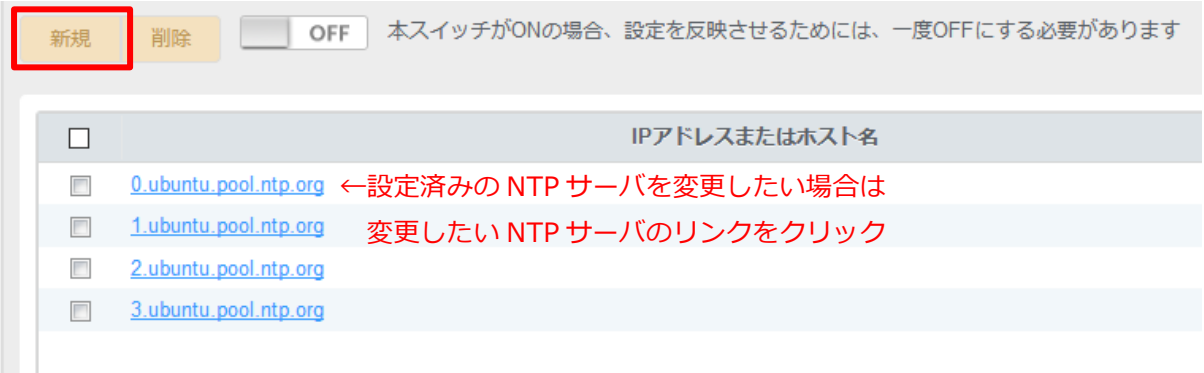
4.2.3. NTP サーバ

1) SYNESIS にサインインします。　※「3.3.1.1 サインイン」参照

2) サインインしたトップ画面の右側上部にある構成アイコン をクリックしてください。

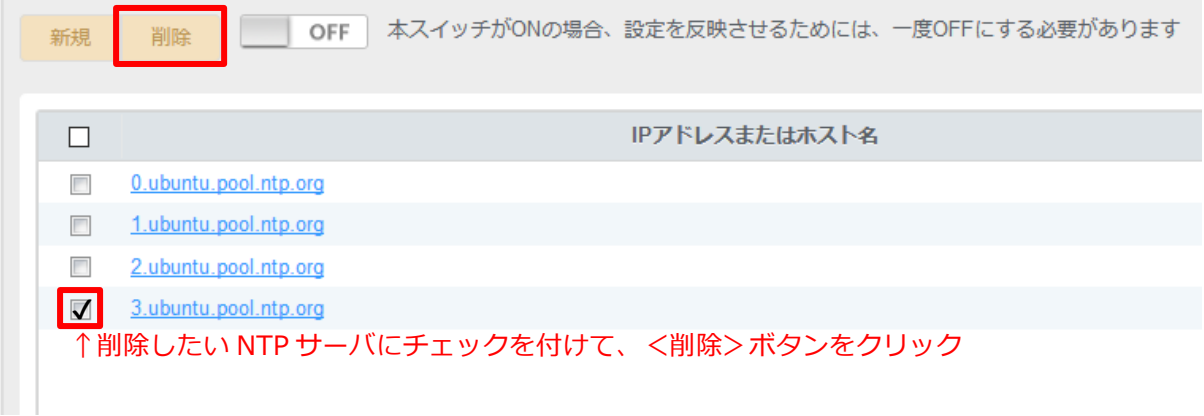
3) [**構成**] 画面が表示されます。左側のメニューの[**構成**] → [**システム**] より [**時刻同期**]を選択してください。

4) [**時刻同期**] 画面が表示されます。NTP サーバを追加する場合は＜**新規**＞ボタンを、設定済みのサーバを変更するには、変更したいサーバをクリックします。



5) 登録(もしくは変更)したい NTP サーバの IP アドレスまたはホスト名を入力して＜**保存**＞ボタンをクリックします。

6) 設定済みのサーバを削除するには、削除したいサーバの左にあるチェックボックスにチェックをして、<**削除**>ボタンをクリックしてください。



7) 確認画面が表示されますので、<**はい**>をクリックしてください。

8) 時刻同期を開始するには、スイッチをクリックして [**ON**] の状態にします。

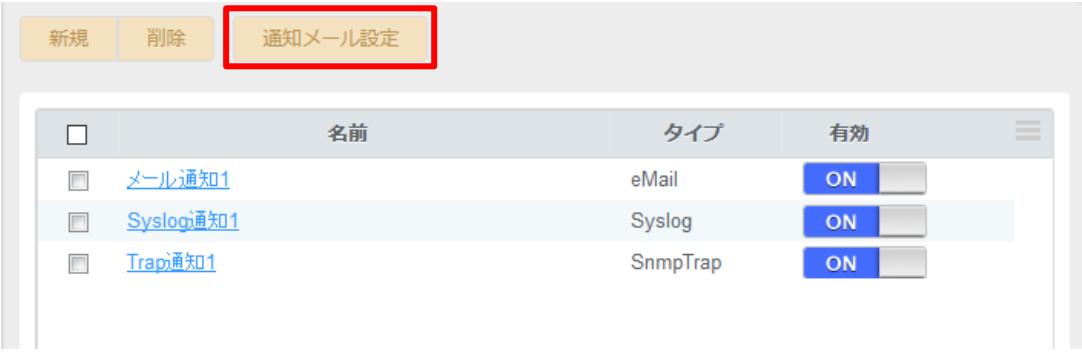
4.2.4. SMTP サーバ

1) SYNESIS にサインインします。 ※「3.3.1.1 サインイン」参照

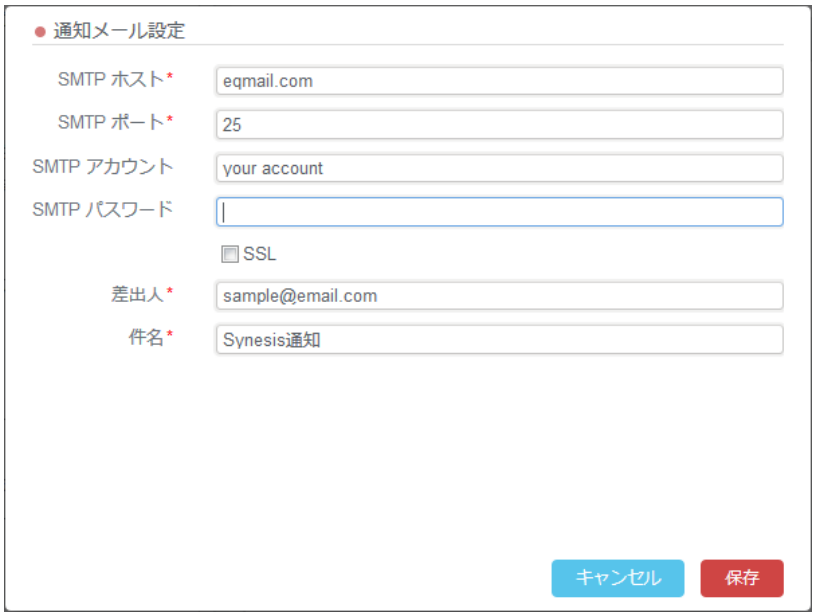
2) サインインしたトップ画面の右側上部にある構成アイコン をクリックしてください。

3) [**構成**] 画面が表示されます。左側のメニュー [**構成**] - [**アラートと通知**] より、[**通知先**] を選択してください。

4) [**通知先**] 画面が表示されます。画面上部の<**通知メール設定**>ボタンをクリックしてください。



5) [**通知メール設定**] 画面が表示されます。SMTP サーバや通知メールに関する設定を変更して、<**保存**>ボタンをクリックしてください。



4.3. iDRAC の初期設定変更

4.3.1. iDRAC ポートのネットワーク設定

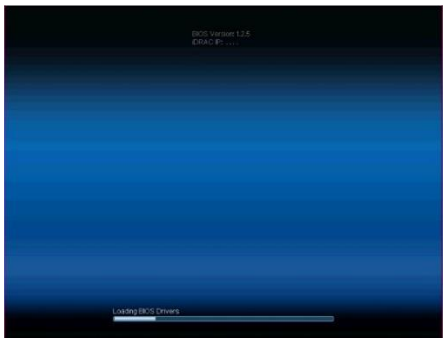
iDRAC の IP アドレスが不明である場合や、iDRAC ポートがネットワークに接続されていない場合は、機器に直接接続されたコンソールを利用して iDRACのネットワーク設定を行ってください。上記条件に該当しない場合は、リモートから iDRAC のネットワーク設定を行うことが可能です。詳細は「4.3.1.2 リモートからの設定」をご参照ください。

4.3.1.1. ローカルコンソールからの設定

ローカルコンソールからの iDRAC のネットワーク設定の変更手順は以下の通りです。

1) SYNESIS を起動、または再起動します。　※「2.1 起動」または「2.3 OS の再起動」参照

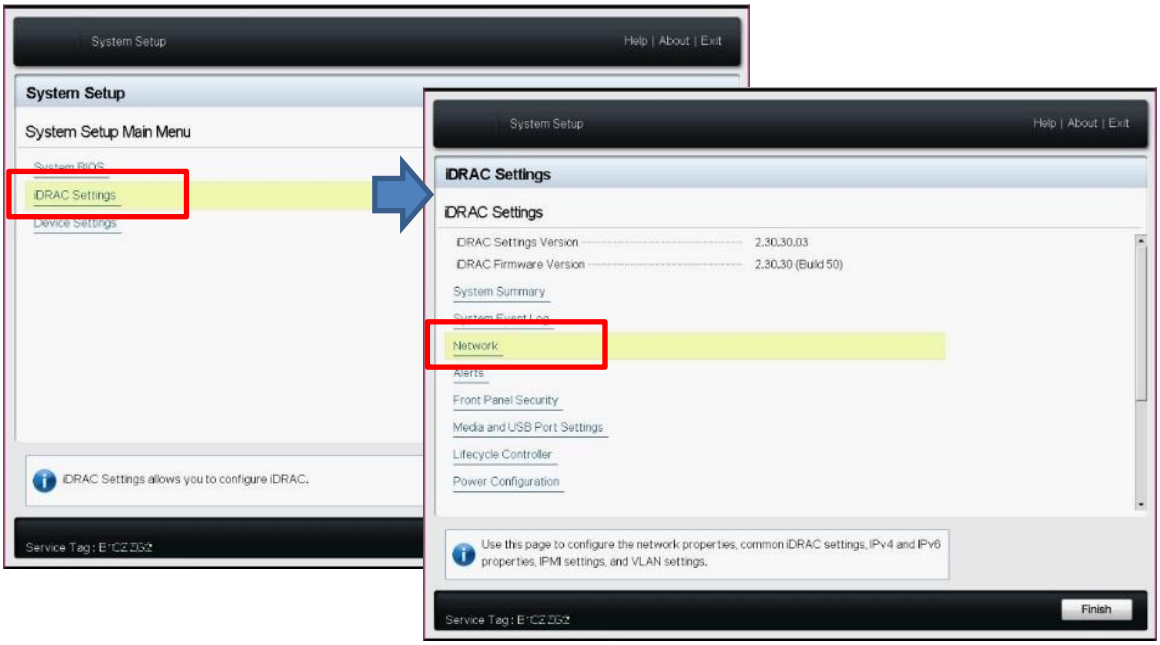
2) 以下のような画面が表示されます。



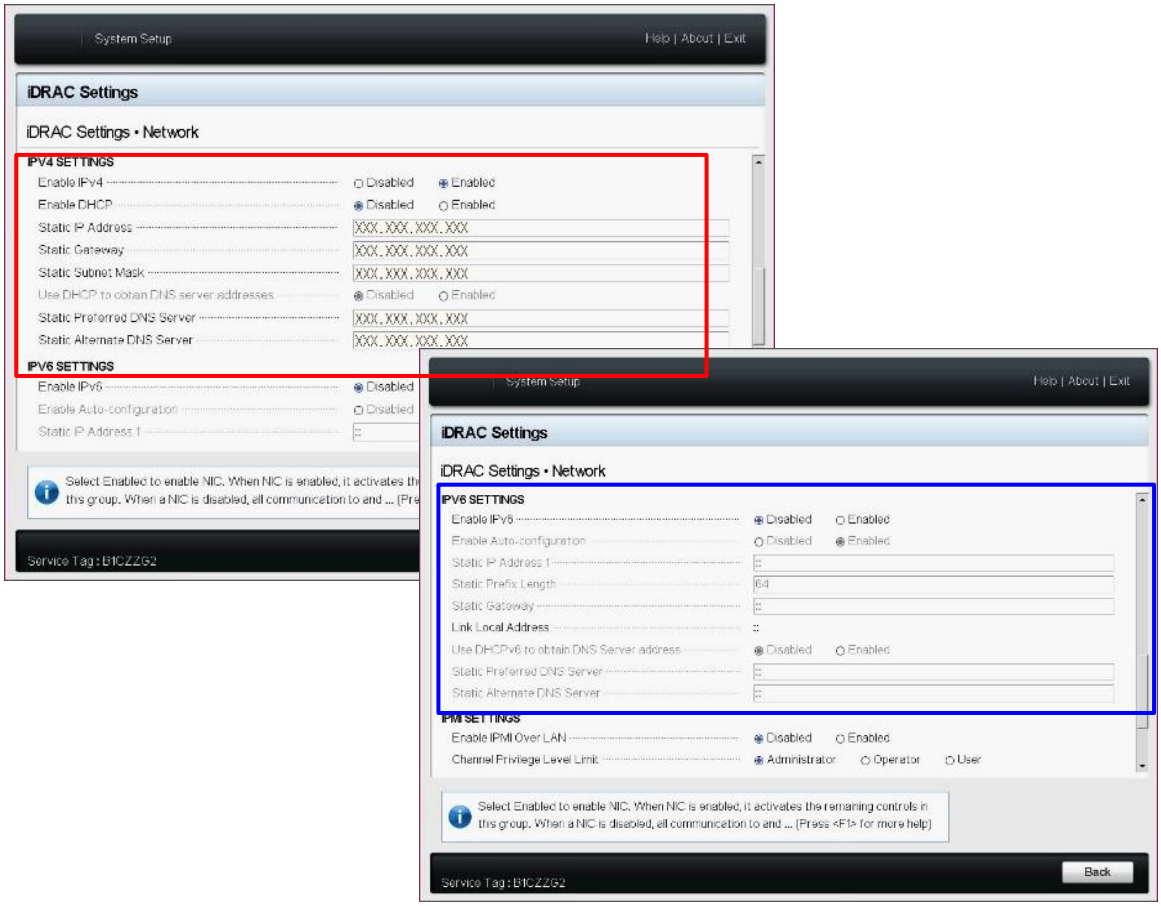
3) 画面上部に以下のような表示が現れたら、キーボードの「F2」を押下してください。

4) 以下のような [**System Setup**] 画面が表示されます。

[**iDRAC Settings**] を選択し、[**iDRAC Settings**] 画面で [**Network**]を選択してください。

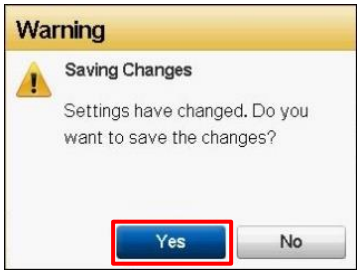


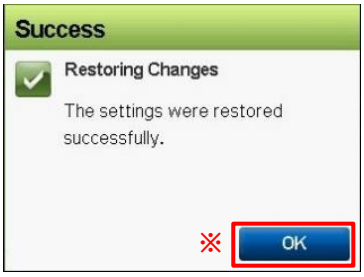
5) [**iDRAC Settings・Network**]画面より、[**IPv4 SETTINGS**](**赤枠**)または[**IPv6 SETTINGS**](**青枠**)の設定を変更し、変更後に右側上部にある<**Exit**>をクリックします。



6) 以下の画面が表示されますので<**Yes**>をクリックしてください。

※変更を取り消す場合は、[**Saving Changes**] 画面で<**No**>をクリックし、[**Restoring Changes**] 画面で<**OK**>をクリックしてください。





7) [**System Setup**] 画面まで戻りますので、右側上部にある<**Exit**>をクリックしてください。

以下の画面が表示されましたら<**Yes**>をクリックしてください。

以上で設定は完了です。必要に応じて iDRAC へログインできることを確認してください。

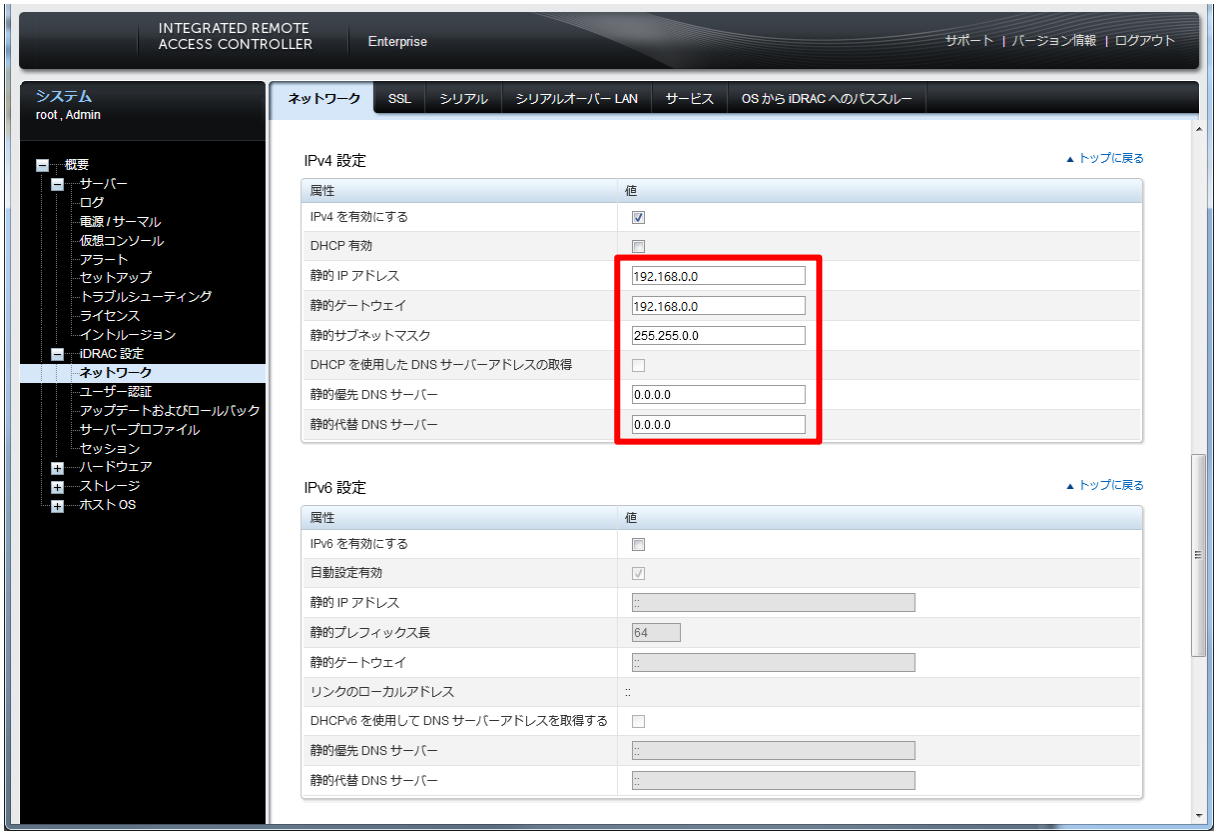
4.3.1.2. リモートからの設定(iDRAC8)

iDRAC8 をご使用の場合の、リモートからの iDRAC ネットワーク設定の変更手順は以下の通りです。

1) iDRAC にログインします。 ※「3.4.1.1 ログイン」参照

2) 画面左側のメニューより [**概要**] – [**iDRAC 設定**] – [**ネットワーク**] を選択してください。

3) [**ネットワーク**] タブの [**IPv4 設定**] または [**IPv6 設定**] にて設定を変更します。



4) 設定後、画面下部にある＜**適用**＞をクリックします

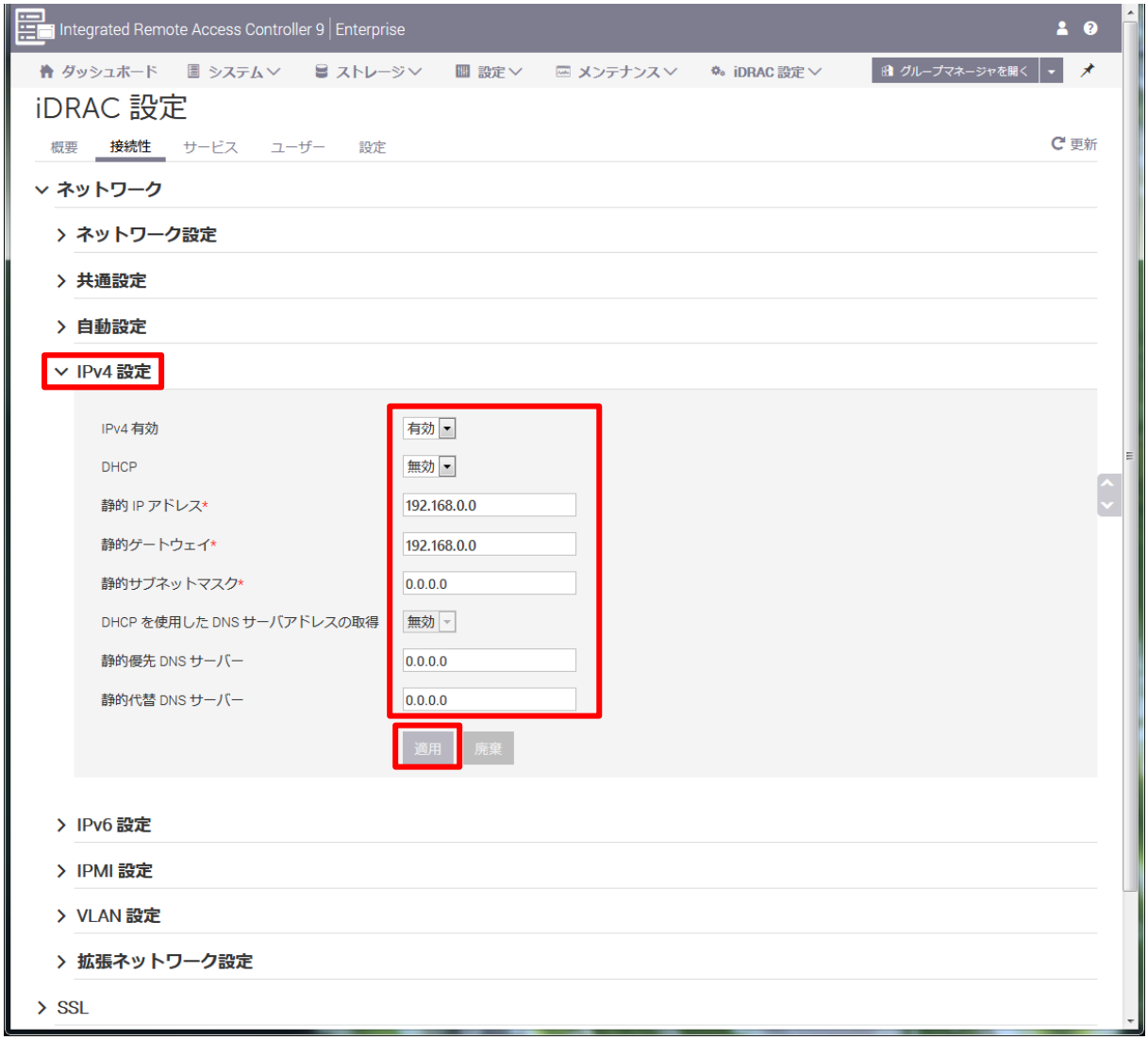
4.3.1.3. リモートからの設定(iDRAC9)

iDRAC9 をご使用の場合の、リモートからの iDRAC ネットワーク設定の変更手順は以下の通りです。

1) iDRAC にログインします。 ※「3.4.2.1 ログイン」参照

2) 画面の上部にあるメニューより [**iDRAC 設定**] - [**接続性**] をクリックします。

3) [**ネットワーク**] – [**IPv4 設定**] または [**IPv6 設定**] にて設定を変更してください。



4) 設定後、画面下部にある<**適用**>をクリックします。

4.3.2. SMTP サーバの設定

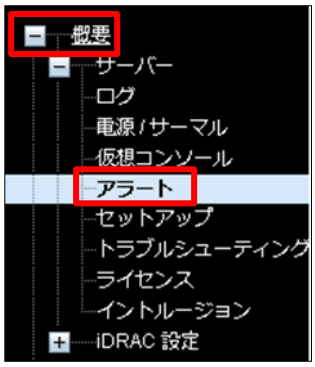
iDRAC からのアラートをメールで通知させたい場合は、SMTP サーバの設定を行ってください。

アラート通知については「6.1. iDRAC：ハードウェアの監視」をご参照ください。

4.3.2.1. iDRAC8

1) iDRAC にログインします。　※「3.4.1.1 ログイン」参照

2) 画面の左側にあるメニューより [**概要**] – [**アラート**] をクリックします。



3) [**SNMP および電子メール設定**] タブの [**SMTP(電子メール)サーバーアドレス設定**] にて設定を変更します。

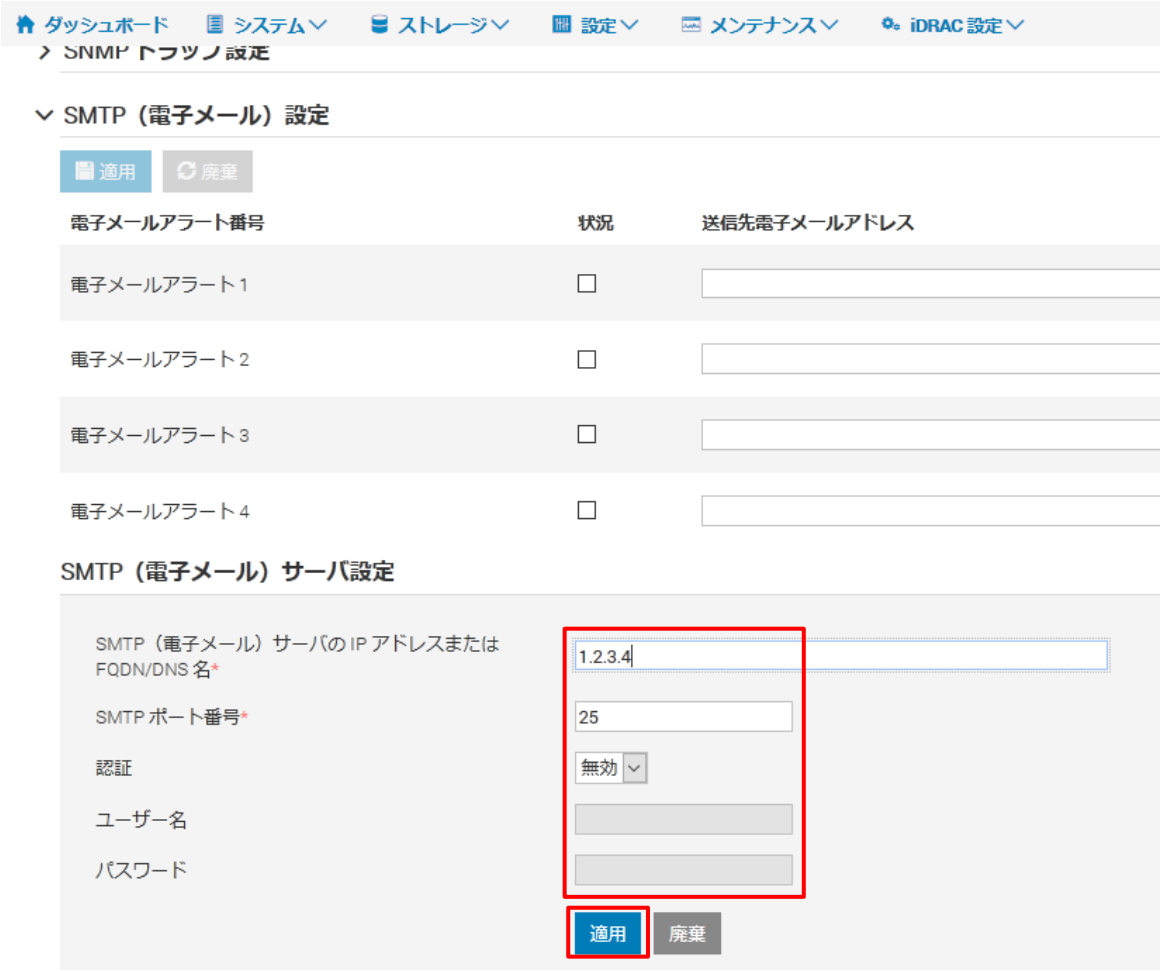
4) 設定後、画面下部にある＜適用＞ボタンをクリックします。

4.3.2.2. iDRAC9

1) iDRAC にログインします。　※「3.4.2.1 ログイン」参照

2) 画面の上部にあるメニューより「設定 -> システム設定」をクリックします。

3) 「SNMP(電子メール)設定」の「SMTP(電子メール)サーバー設定」にて設定を変更し、画面下部にある「適用」をクリックします。



5.アカウント管理

本章では、SYNESIS を運用するのに必要なアカウントの管理方法を説明します。

SYNESIS を構成する 3 つのシステム、OS と SYNESIS、 iDRAC(portable は含まない)に対して、各々アカウントを作成・管理します。

5.1. Ubuntu OS のアカウント

Ubuntu OS のアカウントはローカルの Terminal または SSH から編集することができます。

編集の際には管理者権限のあるユーザでログインしてください。

アカウントに関する制限は以下の通りです。

ユーザ名文字数	16 文字
ユーザ名文字列	アルファベット(a-z)　※大文字は使用不可 数字(0-9) アンダーバー(_) 先頭文字に数字は使用不可
パスワード文字数	16 文字
パスワード文字列	アルファベット(A-Z, a-z) 数字(0-9) 特殊文字(! # $ % & ( ) = - ^ | { } [ ] + * ; : < > , ? _)

5.1.1. Ubuntu OS のアカウント作成

ユーザを新規追加する場合は、以下のコマンドを入力します。

```
⟨ログインユーザ名⟩@⟨ホスト名⟩:~$ sudo□adduser□⟨ユーザ名⟩
[sudo] password for ⟨ログインユーザ名⟩: パスワードを入力
Adding user `⟨ユーザ名⟩' ...
Adding new group `⟨ユーザ名⟩' (1002) ...
Adding new user `⟨ユーザ名⟩' (1002) with group `⟨ユーザ名⟩' ...
Creating home directory `/home/⟨ユーザ名⟩' ...
Copying files from `/etc/skel' ...
Enter new UNIX password: 作成するアカウントのパスワードを入力
Retype new UNIX password: 作成するアカウントのパスワードを入力
passwd: password updated successfully
Changing the user information for ⟨ユーザ名⟩
Enter the new value, or press ENTER for the default
        Full Name []:          ※任意　省略可
        Room Number []:        ※任意　省略可
        Work Phone []:         ※任意　省略可
        Home Phone []:         ※任意　省略可
        Other []:              ※任意　省略可
Is the information correct? [Y/n] y
⟨ログインユーザ名⟩@⟨ホスト名⟩:~$
```

作成したアカウントに管理者権限を与える場合は、以下のコマンドも入力してください。

sudo コマンドが使用できるようになります。

```
⟨ログインユーザ名⟩@⟨ホスト名⟩:~$ sudo□usermod□-G□sudo□⟨ユーザ名⟩
```

5.1.2. Ubuntu OS のアカウント変更

5.1.2.1. ユーザ名の変更

ユーザ名の変更には、そのアカウントとは別の、管理者権限を持つアカウントが必要になります。そのようなアカウントがない場合は、「4.1.2 管理者アカウント(ユーザ名・パスワード)」に従って、一時的なアカウントを作成してください。

作成したアカウントでユーザ名の変更を行い、変更後に作成したアカウントを削除します。

1) 変更したいアカウント以外の管理者権限を持つアカウントでログインします。

2) ユーザ名を変更するには、以下のコマンドを入力します。

```
〈ログインユーザ名〉@〈ホスト名〉:~$ sudo□usermod□-l□<変更後のユーザ名>□<変更前のユーザ名>
[sudo] password for 〈ログインユーザ名〉: パスワードを入力
〈ログインユーザ名〉@〈ホスト名〉:~$ sudo□groupmod□-n□<変更後のユーザ名>□<変更前のユーザ名>
〈ログインユーザ名〉@〈ホスト名〉:~$ sudo□usermod□-d□/home/<変更後のユーザ名>□-m□<変更後のユーザ名>
〈ログインユーザ名〉@〈ホスト名〉:~$ sudo□usermod□-c□<変更後のユーザ名>,,,□<変更後のユーザ名>
```

※以下のファイルで当該アカウントの設定の変更を確認できます。

- /etc/passwd
- /etc/group

3) OS を再起動します。 ※「2.3 OS の再起動」参照

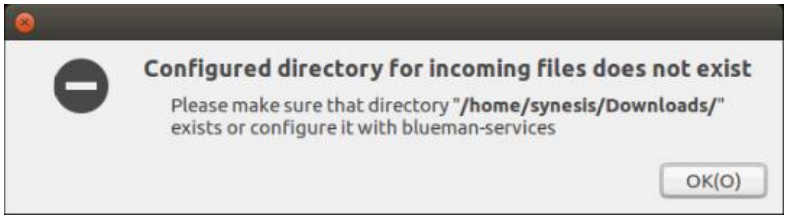
4) 変更されたアカウント(ユーザ名)でログインし、ログイン方法に応じて下記の手順を行います。

[OS のログイン画面よりログインした場合]

5) ログイン後、terminal を開き、以下のコマンドを入力します。

```
<ログインユーザー名>@<ホスト名>:~$
sudo□gsettings□set□org.blueman.transfer□shared-path□"/home/<変更後ユーザ名>/downloads"
```

※ログイン後、下記メッセージが表示されることがありますが、上記コマンドを実施することで、次回ログイン時より表示されなくなります。



[SSH でログインした場合]

5) 以下のコマンドを入力します。

```
〈ログインユーザ名〉@〈ホスト名〉:~$
sudo□dbus-launch□gsettings□set□org.blueman.transfer□shared-path□"/home/
〈変更後ユーザ名〉/downloads"
```

---

6) ユーザ名変更のために、一時的なアカウントを作成している場合は、「5.1.3 Ubuntu OS のアカウント削除」の手順で当該アカウントを削除します。

7) OS を再起動します。 ※「2.3 OS の再起動」参照

5.1.2.2. パスワードの変更

ユーザパスワードを変更する場合は、以下のコマンドを入力します。

```
〈ログインユーザ名〉@〈ホスト名〉:~$ sudo□passwd□〈ユーザ名〉
[sudo] password for 〈ログインユーザ名〉: パスワードを入力
Enter new UNIX password: 変更後アカウントのパスワードを入力
Retype new UNIX password: 変更後アカウントのパスワードを入力
passwd: password updated successfully
〈ログインユーザ名〉@〈ホスト名〉:~$
```

5.1.3. Ubuntu OS のアカウント削除

ユーザを削除する場合は、以下のコマンドを入力します。

```
〈ログインユーザ名〉@〈ホスト名〉:~$userdel□-r□〈ユーザ名〉
[sudo] password for 〈ログインユーザ名〉: パスワードを入力
〈ログインユーザ名〉@〈ホスト名〉:~$
```

5.2. SYNESIS のアカウント

SYNESIS のアカウントには 2 種類あります。 ひとつはメイン GUI 用のアカウントで、キャプチャの実行や分析が行える操作用アカウントになります。 もうひとつはサービス・ログ管理 GUI 用のアカウントで、SYNESIS サービスの操作やログの確認・収集が行えます。

アカウントの作成・管理方法はそれぞれのリンク先をご参照ください。

5.2.1. メイン GUI

SYNESIS に管理者アカウントでサインインしてください。

サインイン後、ツールバー上の構成アイコンをクリックしてください。

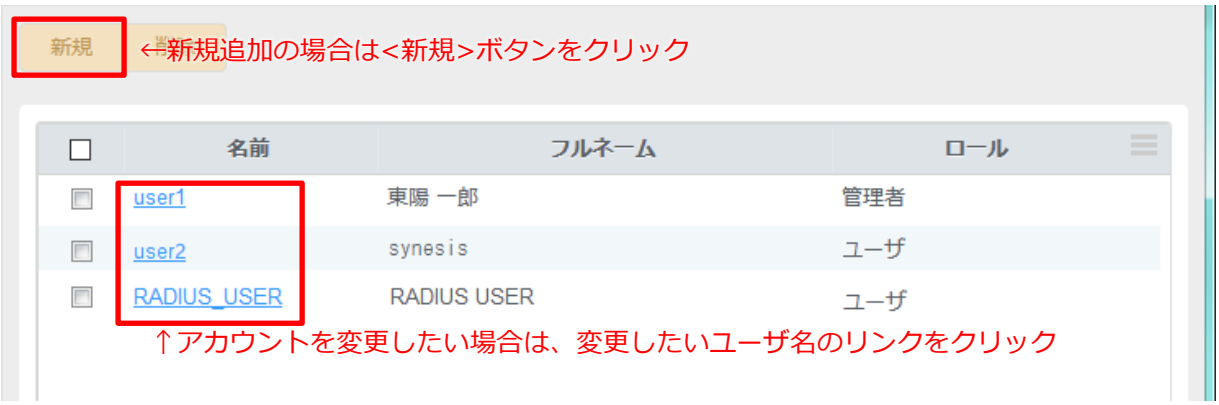
構成メニューの [**システム**] - [**ユーザ**] から、SYNESIS のアカウントの作成・管理が行えます。

アカウントに関する制限は以下の通りです。

同時セッション数	3(デフォルト)
ユーザ名, 姓, 名 文字数	50 25(マルチバイト文字)
ユーザ名, 姓, 名 文字列	下記が利用不可 ! # $ % & = ~ ^ | ¥ ` @ + * , ? (半角) ！ ＃ ＄ ％ ＆ ＝ ～ ＾ ＾ ｜ ¥ ‘ @ ＋ ＊ 、 。 ？ (全角)
パスワード文字数	30 15(マルチバイト文字)
パスワード文字列	下記が利用不可 ! # $ % & = ~ ^ | ¥ ` @ + * , ? (半角) ！ ＃ ＄ ％ ＆ ＝ ～ ＾ ＾ ｜ ¥ ‘ @ ＋ ＊ 、 。 ？(全角)
ロール	管理者：制限なし ユーザ：主に解析・参照機能のみ利用可能

5.2.1.1. SYNESIS メイン GUI のアカウント作成・変更

1) アカウントを新規追加する場合は、<**新規**>ボタンをクリックします。
アカウントを変更する場合は、変更したいユーザ名をクリックします。

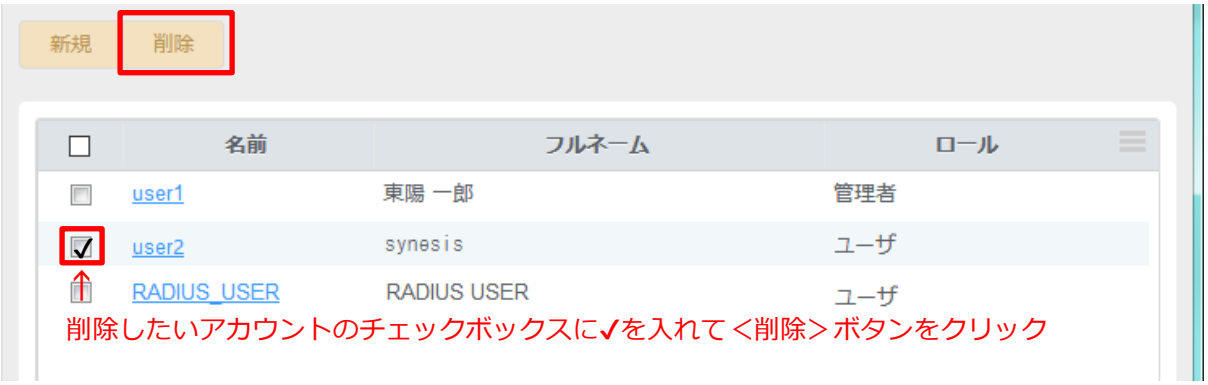


2) ユーザープロファイル画面が表示されます。必要事項を入力して、<**保存**>ボタンをクリックしてください。

5.2.1.2. SYNESIS メイン GUI のアカウント削除

1) アカウントを削除する場合は、削除したいユーザ名にチェックを入れてください。
※ラベル欄のチェックボックスをクリックすると、全てのユーザが選択されます。

2) <**削除**>ボタンをクリックします。削除確認のダイアログが表示されますので、<**はい**>をクリックしてください。



5.2.2. サービス・ログ管理 GUI

SYNESIS のローカルから Terminal を起動するか、リモートから SSH で接続します。

※「3.2.2 SSH」参照

アカウントに利用可能な文字数、文字列に関する制限は以下の通りです。

項目	制限
ユーザー名・ パスワード文字数	16 文字まで
ユーザー名・ パスワード文字列	アルファベット(A-Z, a-z) 数字(0-9) 特殊文字(! # % & ( ) = ~ | - ^ ¥ { } [ ] @ + * ; < > , . ? _ / ¥)

5.2.2.1. SYNESIS サービス・ログ管理 GUI のアカウント作成・変更

1) 以下のコマンドを入力し、追加・変更したいユーザーとそのパスワードを指定します。

```
コマンド：$sudo□su□-
コマンド：#htpasswd□/etc/nginx/synesis/.htpasswd□〈ユーザ名〉
          New Password:          〈パスワード〉
          Re-type new password:  〈パスワード〉
```

2) 以下のコマンドを入力し、変更した設定を読み込みます。

```
コマンド：#nginx□-t
コマンド：#nginx□-s□reload
```

5.2.2.2. SYNESIS サービス・ログ管理 GUI のアカウント削除

1) 以下のコマンドを入力し、エディタにて削除したいユーザーが記載されている行を削除します。

```
コマンド：$sudo□su□-
コマンド：#vi□/etc/nginx/synesis/.htpasswd
```

例：ユーザー”test1”を削除したい場合

```
synesis@for_example:~$ sudo su -
[sudo] password for synesis: パスワードを入力
synesis@for_example:~# vi /etc/nginx/synesis/.htpasswd
example:$apr1$xfAVfaqh$XR/alY.lSI3cieO9MV6de0
test1:$apr1$qMdKa3f6$py5EU9GsUoJQGzlsX4q2a0
test2:$apr1$B5L9jXBU$kWhnws.28mxX6Ii003stc0
```

この行を削除します。その後以下を入力してエディタを終了します。

:wq

2) 以下のコマンドを入力し、変更した設定を読み込みます。

```
コマンド：#nginx□-t
コマンド：#nginx□-s□reload
```

5.3. iDRAC のアカウント

iDRAC のアカウントを iDRAC の GUI から編集することができます。

アカウントに関する各制限は以下の通りです。

項目	制限
最大設定ユーザー数	15
ユーザー名文字数	16 文字 ※空白を含む
ユーザー名文字列	アルファベット(A-Z, a-z) 数字(0-9) 特殊文字(! # $ % & ( ) = - ^ | { } [ ] + * ; : < > , ? _ § I)
パスワード文字数	20 文字
パスワード文字列	アルファベット(A-Z, a-z) 数字(0-9) 特殊文字(! " # $ % & () = - | { } [ ] @ + * ; : < > , . ? _ / ¥ § I)

iDRAC のアカウントの登録・編集方法は iDARC8 と iDRAC9 で異なります。

ログイン画面に表示される、[Integrated Dell Remote Access Controller] の最後の数字を確認し、「8」の場合は「5.3.1.iDRAC8」を、「9」の場合は、「5.3.2.iDRAC9」をご参照ください。

5.3.1. iDRAC8

iDRAC8 のアカウント登録・編集 GUI へのアクセス方法は以下の通りです。

1) iDRAC に管理者アカウントでログインします。 ※「3.4.1.1 ログイン」参照

2) [**概要**] - [**iDRAC 設定**] - [**ユーザー認証**] と選択してください。

[**ユーザー認証**] 画面が表示されます。

5.3.1.1. iDRAC のアカウント作成

1) 使用されていないユーザーの [**ユーザーID 番号**] をクリックします。

2) [**ユーザーの設定**] を選択し、<**次へ**>ボタンをクリックします。

3) [**一般**] 欄にて、ユーザー名、パスワードを入力し、[**iDRAC ユーザー特権**]欄にて役割を選択して、<**適用**>ボタンをクリックします。

5.3.1.2. iDRAC のアカウント変更

1) 変更したいユーザーの [**ユーザーID 番号**] をクリックしてください。

2) [**ユーザーの設定**] を選択し、<**次へ**>ボタンをクリックしてください。

3) 設定を適宜変更し、<**適用**>ボタンをクリックします。

パスワードを変更する場合は、[**パスワードの変更**] チェックボックスをチェックします。

5.3.1.3. iDRAC のアカウント削除

1) [**ローカルユーザ**]欄のユーザリストで削除したいユーザーの[**ユーザーID 番号**]をクリックします。

2) [**ユーザーの設定**] を選択し、<**次へ**>ボタンをクリックします。

3) [**ユーザーを有効にする**] 欄のチェックボックスのチェックを外し、<**適用**>ボタンをクリックしてください。

5.3.2. iDRAC9

iDRAC9 のアカウント登録・編集 GUI へのアクセス方法は以下の通りです。

1) iDRAC に管理者アカウントでログインします。 ※「3.4.2.1 ログイン」参照

2) [**iDRAC 設定**] - [**ユーザー**]と選択してください。

3) [**ユーザー**] 画面が表示されます。[**ローカルユーザ**] 欄を開いてください。

5.3.2.1. iDRAC のアカウント作成

1) [**ローカルユーザ**] 欄の＜**追加**＞ボタンをクリックしてください。

2) ユーザー名、パスワードを入力し、＜**保存**＞ボタンをクリックしてください。

必要があれば [**ユーザー特権**] 欄にて役割を指定してください。

5.3.2.2. iDRAC のアカウント変更

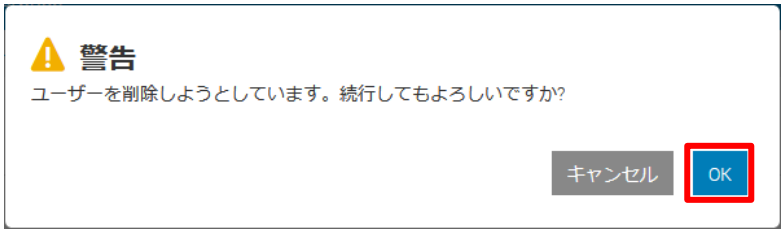
1) [**ローカルユーザ**] 欄のユーザリストから変更したいユーザーを選択し <編集> をクリックします。

2) 設定を適宜変更し、「保存」ボタンをクリックします。

5.3.2.3. iDRAC のアカウント削除

1) [**ローカルユーザ**] 欄のユーザリストから削除したいユーザーを選択し <**削除**> をクリックします。

2) 以下のような確認のメッセージが表示されますので、 <**OK**> をクリックしてください。



6.SYNESIS の監視機能

本章では、SYNESIS の監視機能を説明します。監視できる内容は、SYNESIS を構成するソフトウェアごとに異なり、それぞれ下記のようになっております。

- iDRAC：ハードウェアの異常監視（SYNESIS Portable は除く）
- SYNESIS ソフトウェア：キャプチャ動作中の異常監視、キャプチャトラフィックの状態監視

6.1. iDRAC：ハードウェアの監視

iDRAC により SYNESIS のハードウェア状態を監視できます。（SYNESIS Portable は除く）

また、ハードウェアに関するイベント発生時に SNMP トラップや電子メールで通知させることも可能です。

なお、iDRAC の操作方法は iDARC8 と iDRAC9 で異なります。

ログイン画面に表示される、[Integrated Dell Remote Access Controller] の最後の数字を確認し、「８」の場合は「6.1.1.iDRAC8」を、「９」の場合は、「6.1.2.iDRAC9」をご参照ください。

6.1.1. iDRAC8

6.1.1.1. ハードウェア状態の確認

1) iDRAC に管理者アカウントでログインしてください。　※「3.4.1.1 ログイン」参照
2) 画面左側のメニューで[**概要**] – [**サーバー**] を選択してください。
3) [**サーバーの正常性**] 欄を確認してください。

主要な監視項目は下図の通りです。　※製品タイプによりハードウェアに差異があります

アイコンが ⊗ になっている場合は、ハードウェアに異常が発生しています。

6.1.1.2. ハードウェアイベントの通知

どのイベントが発生した時にどの通知先に通知するか、通知手段と通知先をイベント別に設定することができます。まず SNMP トラップやメールアドレスなどの通知手段別に通知先を登録し、その後、通知内容(イベント)と通知手段の設定を行ってください。

6.1.1.2.1. 通知先の設定

1) iDRAC に管理者アカウントでログインしてください。 ※「3.4.1.1 ログイン」参照

2) [**概要**] – [**サーバー**]- [**アラート**] を選択します。

3) [**SNMP および電子メール設定**] タブ を選択してください。

[SNMP Trap で通知する場合]

4) [**IP 送信リスト**] の「アラート送信先 1 (登録済みの場合は 2 以降で可)」を選択し、下記項目を設定します。

- 選択した行の [**状況**] にチェックを入れる
- [**送信先アドレス**] 欄に SNMP マネージャー(送信先)の IP アドレスを入力

5) [**コミュニティ文字列**] に任意のコミュニティ名を入力し、<**適用**>ボタンをクリックします。

6) [**SNMP トラップフォーマット**] 欄にて任意のフォーマットを選択してください。

7) 選択後、[**SNMP トラップフォーマット**] 欄の<**適用**>ボタンをクリックしてください。

[電子メールで通知する場合]

3) SMTP サーバ SMTP サーバの設定が済んでいることを確認します。　※「4.3.2 SMTP サーバの設定」参照

4) [**送信先電子メールアドレス**] の「電子メールアラート 1 (登録済みの場合は 2 以降で可)」を選択し、下記項目を設定します。

- 選択した行の [**状況**] にチェックを入れる
- [**送信先電子メールアドレス**] に送信したいメールアドレスを入力

5) 設定後、<**適用**>ボタンをクリックしてください。

6.1.1.2.2. 通知内容・通知手段の設定

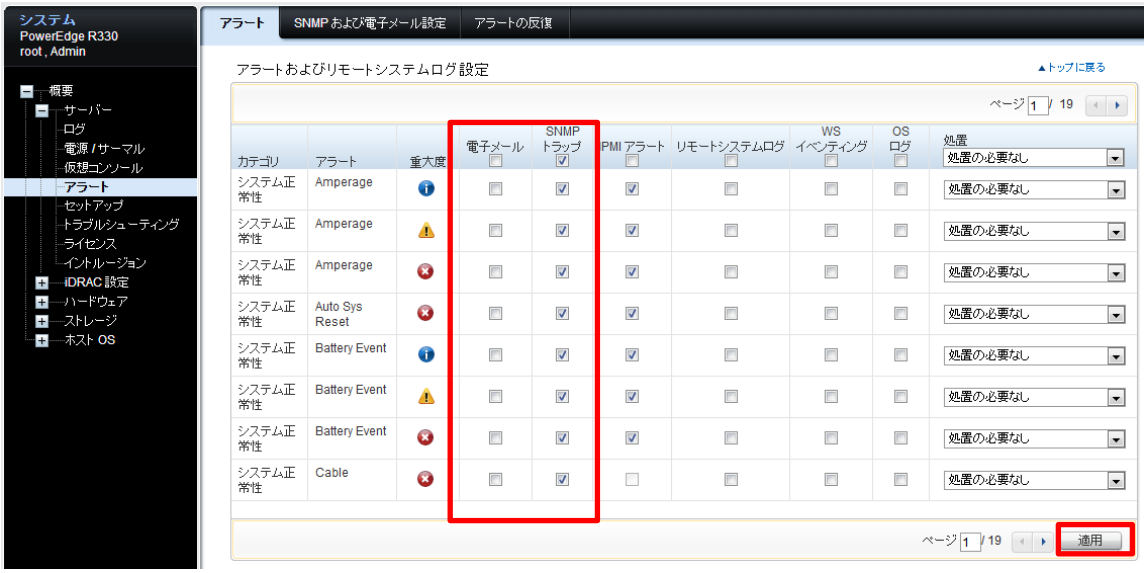
1) iDRAC に管理者アカウントでログインしてください。　※「3.4.1.1 ログイン」参照

2) 画面左側のメニューで[**概要**] - [**サーバー**] - [**アラート**] を選択してください。

3) [**アラート**] タブを選択してください。

4) [**アラート**] 項目にて [**有効**] を選択し、<**適用**>ボタンをクリックします。

5) [**アラートおよびリモートシステムログ設定**] 項目にて、発生時に通知を行いたいイベントと通知手段(SNMP Trap/電子メール)を設定します。



6) 設定後、<**適用**>ボタンをクリックしてください。

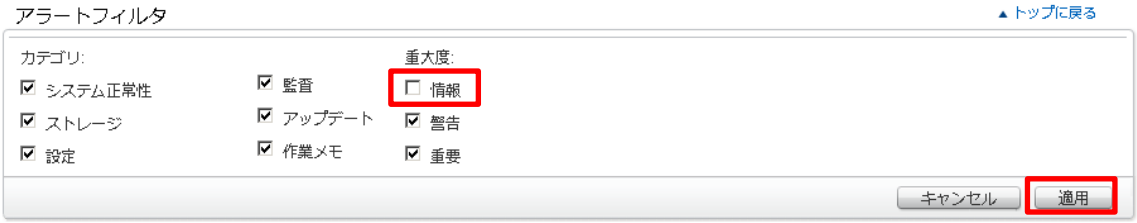
【重大度「警告」と「重要」のイベントを通知する場合】

[**アラート**] タブ画面にはイベントの一覧が表示されています。

どのイベントを通知させるべきか判断に迷う場合は、重大度が「警告」と「重要」であるイベントを選択することを推奨いたします。

「警告」と「重要」のイベントを選択する場合は、7) 以降の手順に従ってください。

7) [**アラート**] タブの [**アラートフィルタ**] 項目にて、重大度 [**情報**] のチェックを外し、<**適用**>ボタンをクリックします。



8) [**アラートおよびリモートシステムログ設定**] 項目にて、以下の手順を繰り返し、表示された全てのイベントに対して通知手段を設定します。

イベントリストが複数ページ表示されますので、各ページで以下の作業を行ってください。

- 利用したい [**通知手段**] をチェックし、表示されているイベント全てにチェックをつけます
- 次のページへ移動します

9) 全てのイベントに対して通知手段を設定できたら、<**適用**>ボタンをクリックします。

6.1.2. iDRAC9

6.1.2.1. ハードウェア状態の確認

1) iDRAC に管理者アカウントでログインしてください。 ※「3.4.2.1 ログイン」参照

2) 以下の [**ダッシュボード**] 画面が表示されます。[**正常性情報**] 欄を確認してください。

アイコンが ⊗ になっている場合は、ハードウェアに異常が発生しています。詳細は「詳細」または、表示された項目をクリックすることで確認することができます。

6.1.2.2. ハードウェアイベントの通知

どのイベントが発生した時にどの通知先に通知するか、通知手段と通知先をイベント別に設定することができます。まず SNMP トラップやメールアドレスなどの通知手段別に通知先を登録し、 その後、通知内容(イベント)と通知手段の設定を行ってください。

6.1.2.2.1. 通知先の設定

1) iDRAC に管理者アカウントでログインしてください。 ※「3.4.2.1 ログイン」参照

2) 画面上部のメニューから [**設定**] – [**システム設定**] を選択します。

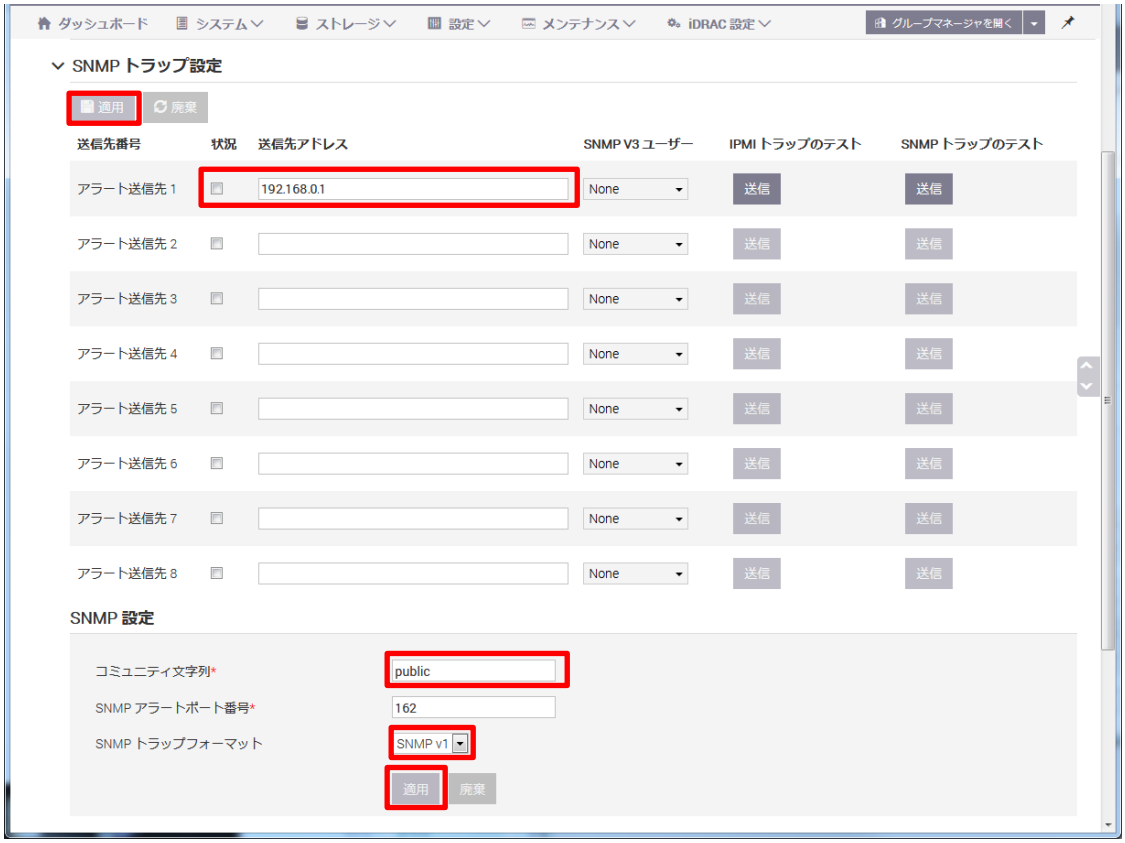
[SNMP Trap で通知する場合]

3) [**アラート設定**] – [**SNMP トラップ設定**] を開きます。

4) 「アラート送信先 1 (登録済みの場合は 2 以降で可)」を選択し、下記項目を設定してください。

- 選択した行の [**状況**] にチェックを入れる
- [**送信先アドレス**] に SNMP マネージャー(送信先)の IP アドレスを入力

5) 設定後、[**SNMP トラップ設定**] 欄の <**適用**> ボタンをクリックしてください。



6) [**SNMP 設定**] 欄にて下記項目を設定し、 <**適用**> ボタンをクリックしてください。

- [**コミュニティ文字列**] に任意のコミュニティ名を入力
- [SNMP トラップフォーマット] にてフォーマットを選択

[電子メールで通知する場合]

3) SMTP サーバの設定が済んでいることを確認します。 ※「4.3.2 SMTP サーバの設定」参照

4) [**アラート設定**] – [**SMTP(電子メール)設定**] を開きます。

5) 「電子メールアラート 1 (登録済みの場合は 2 以降で可)」の下記項目を設定してください。

- 選択した行の [**状況**] にチェックを入れる
- [**送信先電子メールアドレス**」に送信したいメールアドレスを入力

6) 設定後、[**SMTP(電子メール)設定**] 欄の <適用> ボタンをクリックします。

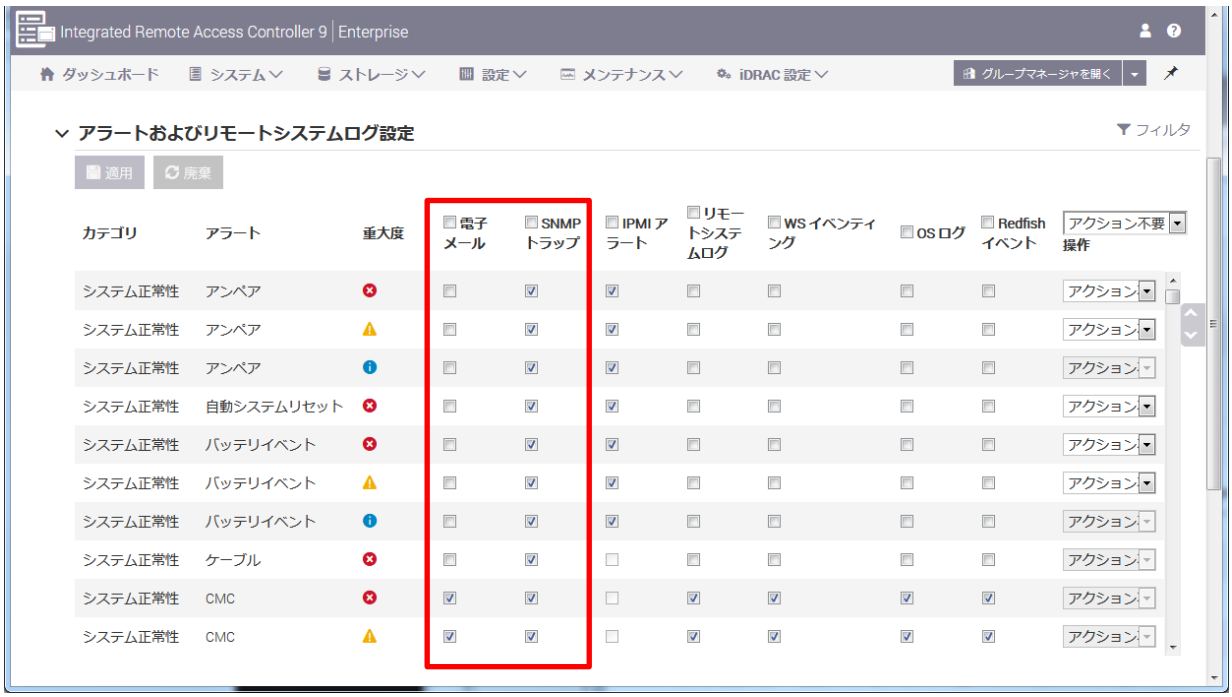
6.1.2.2.2.　通知内容・通知手段の設定

1)　iDRAC に管理者アカウントでログインしてください。　※「3.4.2.1 ログイン」参照

2)　画面上部のメニューから [**設定**] – [**システム設定**] を選択します。

3)　[**アラート設定**] の [**アラート**] 欄で [**有効**] を選択し、<**適用**>ボタンをクリックしてください。

4)　[**アラートおよびリモートシステムログ設定**] 欄を開き、発生時に通知を行いたいイベントと通知手段(SNMP Trap/電子メール)を設定します。



画面にはイベントの一覧が表示されています。通知を行いたいイベントにて、利用したい通知手段(SNMP Trap/電子メール)にチェックをして、<**適用**>ボタンをクリックしてください。

どのイベントを通知すべきか判断に迷う場合は、重大度が「警告」と「重要」であるイベントを通知することを推奨いたします。「警告」と「重要」のイベントを選択する場合は、次ページの「重大度『警告』と『重要』のイベントを通知する場合」をご参照ください。

【重大度「警告」と「重要」のイベントを通知する場合】

5)　[**フィルタ**]をクリックし、重大度 [**情報**] のチェックを外します。

6)　<**適用**>ボタンをクリックしてください。

イベント一覧に重大度が「警告」と「重要」であるイベントだけが表示されます。

7)　利用したい通知手段にチェックをつけ、表示されているイベント全てにチェックをつけます。

8)　全てのイベントに対して通知手段を設定できたら、<**適用**>ボタンをクリックします。

6.2. SYNESIS ソフトウェア：キャプチャ動作中の異常監視

SYNESIS ソフトウェアでは、キャプチャ動作中に以下の項目の状態を監視し、イベント発生時に通知を出すことができます。

監視項目	内容
自動保存	自動保存の失敗と保存先の切り替えを通知
リンクステータス	キャプチャポートのリンクステータスの変化を通知
ドロップ	キャプチャ中のドロップパケット発生を通知

SNMP トラップやメールアドレスなど、通知手段ごとに通知先を登録し、登録した通知先を通知グループに登録します。イベント発生の通知をどこに出すかは、イベントごとに通知グループで指定しできます。

通知先・通知グループの登録方法は「6.2.1 通知先、通知手段の設定」を、 イベント発生の通知先(通知グループ)の指定方法は「6.2.2 通知するイベントの設定」を参照してください。

6.2.1. 通知先、通知手段の設定

SNMP トラップやメールアドレスなど、通知手段ごとに通知先を登録して、登録したそれらの通知先を通知グループに登録する手順は以下の通りです。

1) SYNESIS に管理者アカウントでサインインします。 ※「3.3.1.1 サインイン」参照

2) ツールバーの構成 アイコンをクリックしてください。

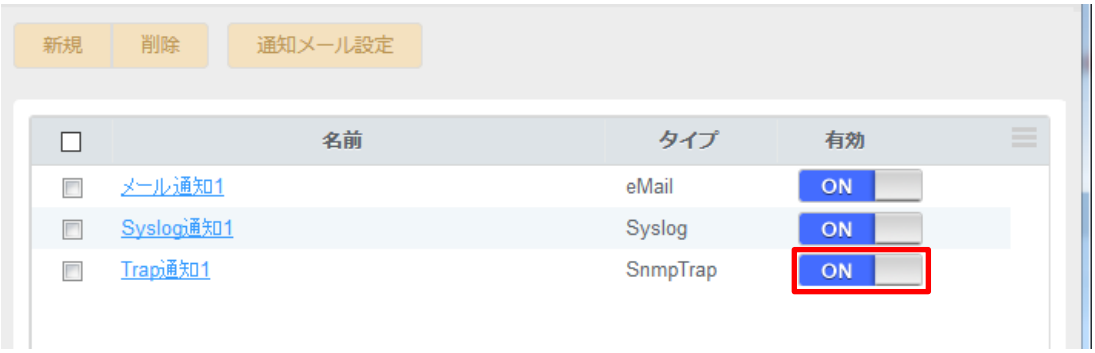
3) [**構成**] メニューが表示されます。[**アラートと通知**]→[**通知先**] を選択してください。

4) [**通知先**] 画面が表示されます。画面上部の＜**新規**＞ボタンをクリックしてください。

5) 通知先登録画面が表示されます。

通知手段を選択し、通知先を設定して、<**保存**>ボタンをクリックしてください。設定した通知先がリストに追加されます。

6) 設定した通知先の [**有効**] 欄が ON になっていることを確認してください。



7) 続いて [**通知先**] で登録した個々の通知先を通知グループに登録します。

[**構成**] → [**アラートと通知**] → [**通知グループ**] を選択してください。

8) [**通知グループ**] 画面が表示されます。画面上部にある [**新規**] ボタンをクリックしてください。

9) 通知グループ登録のダイアログが表示されます。以下の項目を設定してください。

- [**名前**] 欄に登録したい通知グループのグループ名を入力
- [**通知先**] 欄でグループに登録したい通知先(複数可)を選択

左側の欄に登録済みの通知先が表示されます。

左側の欄から登録したい通知先を選択し、>> ボタンをクリックしてください。 選択した通知先が右の欄に移動します。右側の欄にリストアップされた通知先がその通知グループに登録されます。

10) 設定後、 <**保存**> ボタンをクリックしてください。

11) 設定した通知グループが一覧に追加されます。必要に応じて <**通知テスト**> ボタンをクリックして、通知テストを実行してください。

※「通知テスト」は通知の送信が実行できるかのテストになります。無事、通知が受信されたかどうかは受信側でご確認ください。

6.2.2. 通知するイベントの設定

監視項目ごとに、イベントの発生が検出された際に通知を行うか否か、通知を行う場合はどの通知先(通知グループ)に通知するかを設定できます。

設定手順は以下の通りです。

1) SYNESIS に管理者アカウントでサインインします。 ※「3.3.1.1 サインイン」参照

2) 画面左端のメイン・メニューリストから [**エージェント**] を選んでクリックしてください。

3) [**概要**] タブの<**オプション**>ボタンをクリックしてください。

キャプチャオプション画面が表示されますので、[**通知設定**] タブを選択してください。

4) 通知したいイベントの [**有効**] にチェックし、通知先(設定済みの通知グループ)を選択した上で、<**適用**>ボタンをクリックします。

6.3. SYNESIS ソフトウェア：キャプチャトラフィックの状態監視

SYNESIS ソフトウェアでは、キャプチャしたトラフィクについて下記項目の状態を監視し、予め設定した閾値を超えた場合にアラートを発生・記録します。アラート発生時には併せて通知を出すことができます。

アラートを設定可能な項目は以下の通りです。

カテゴリ	サンプリング	検出単位	(自動)解析の要否	監視項目
DLC	1 秒	チャネル毎	不要	総パケット(pps)
				双方向ビットレート(kbps)
ARP	1 分	チャネル合計	必要	パケット(pps)
NPM	1 分	チャネル合計	必要	総パケット(pps)
				双方向ビットレート(kbps)
				受信パケット(pps)
				受信ビットレート(kbps)
				送信パケット(pps)
				送信ビットレート(kbps)
APM	1 分	チャネル合計	必要	ART(ミリ秒)
				PTT(ミリ秒)
				NRT(ミリ秒)
				SRT(ミリ秒)
				CRT(ミリ秒)
				遅延(ミリ秒)
				リトライ(回数)

- サンプリングは、検出間隔です
- カテゴリによっては、キャプチャしたトラフィックの解析が必要です

※用語については、SYNESIS ユーザーガイドを参照してください。

6.3.1. アラートの設定

アラートを発生させるための閾値と、そのアラートが発生した場合の通知先を設定できます。

アラートの通知先はアラートごとに、登録済みの通知先から選択可能です。 通知先の登録方法は「6.2.1.通知先、通知手段の設定」をご参照ください。

アラートの設定方法は以下の通りです。

1) SYNESIS に管理者アカウントでサインインします。 ※「3.3.1.1 サインイン」参照

2) ツールバーの構成アイコンをクリックしてください。

3) [**構成**] メニューが表示されます。[**アラートと通知**] - [**アラート**] を選択してください。

4) アラートを発生させたい項目が属するカテゴリのタブ(DCL, ARP, NPM, APM)を選択し、<**新規**>ボタンをクリックしてください。

5) アラート登録画面が表示されます。閾値、通知先などを設定して、<**保存**>ボタンをクリックしてください。

6) 設定したアラームが一覧に追加されます。通知先の登録方法は「6.2.1.通知先、通知手段の設定」をご参照ください。

7) 追加されたアラートの [**有効/無効**] 欄が ON になっていることを確認してください。

7.設定情報やデータのバックアップ

SYNESIS の設定やデータのバックアップを取り、故障回復後やリカバリ後に設定やデータを復元(リストア)することが可能です。

バックアップ可能なのは OS の設定情報や SYNESIS の設定情報、 トレース・ファイル、作成されたレポートです。 キャプチャ・データは直接バックアップを取ることができません。 キャプチャ・データをトレース・ファイルに保存し直してバックアップを行います。

バックアップ方法はそれぞれのリンク先を、復元(リストア)方法の詳細は 8. 設定情報やデータのリストアをご参照ください。

7.1. OS 設定情報のバックアップ

OS の設定内容については、OS がインストールされているディスク(デバイスファイル)を、バックアップ・ツールなどを利用して丸ごとバックアップします。

OS がインストールされているディスク(デバイスファイル名：/dev/sda, /dev/sdb など)は、df コマンド等で確認することができます。

バックアップ作成手順は以下の通りです。

1) SYNESIS へ SSH で接続します。 ※「3.2.2 SSH」参照

2) 以下のコマンドで、OS がインストールされているディスク(デバイスファイル名)を確認します。

コマンド：df

```
[redacted]:~$ df
Filesystem      1K-blocks      Used Available Use% Mounted on
udev             16395552         0  16395552   0% /dev
tmpfs             3283176      9876   3273300   1% /run
/dev/sda1       925170212   8520868 872527536   1% /
tmpfs            16415868         8  16415860   1% /dev/shm
tmpfs                5120         4      5116   1% /run/lock
tmpfs            16415868         0  16415868   0% /sys/fs/cgroup
/dev/sdb        975737352     32928 975704424   1% /pvc/data/databank
/dev/sdg        156160400[redacted]
/dev/sde        156160400[redacted]
/dev/sdc        156160400[redacted]
/dev/sdd        156160400[redacted]
/dev/sdh        156160400[redacted]
/dev/sdi        156160400[redacted]
/dev/sdf        156160400[redacted]
tmpfs             3283176         0   3283176   0% /run/user/1000
```

「/」へマウントされているデバイスファイル名(数値を除く)を確認します。

本例の場合：/dev/sda

3) 手順 2)で確認した、OS がインストールされているディスクからシステムイメージを作成するなどして、丸ごとバックアップしてください。

7.2. SYNESIS 環境・設定情報

SYNESIS の設定情報としてライセンス・ファイルと 構成(コンフィグ)情報のコンフィグ・ファイルの バックアップファイルを作成することが可能です。

なお、マザー・ボードの故障などにより eth ポートの MAC アドレスが変更された場合は、バックアップしたライセンスは利用できません。 ライセンスの再発行が必要となりますので、弊社サポート宛にご連絡ください。

7.2.1. ライセンス・ファイルのバックアップ

ライセンス・ファイルのバックアップ手順は以下の通りです。

1) SYNESIS へ SSH で接続します。 ※「3.2.2 SSH」参照

2) SCP などを利用して、以下の場所にあるライセンス・ファイルを SYNESIS 外の外部ストレージなどにバックアップ(保存)してください。

場所：/var/lib/tomcat7/pvclicense.lic

7.2.2. コンフィグ・ファイルのバックアップ

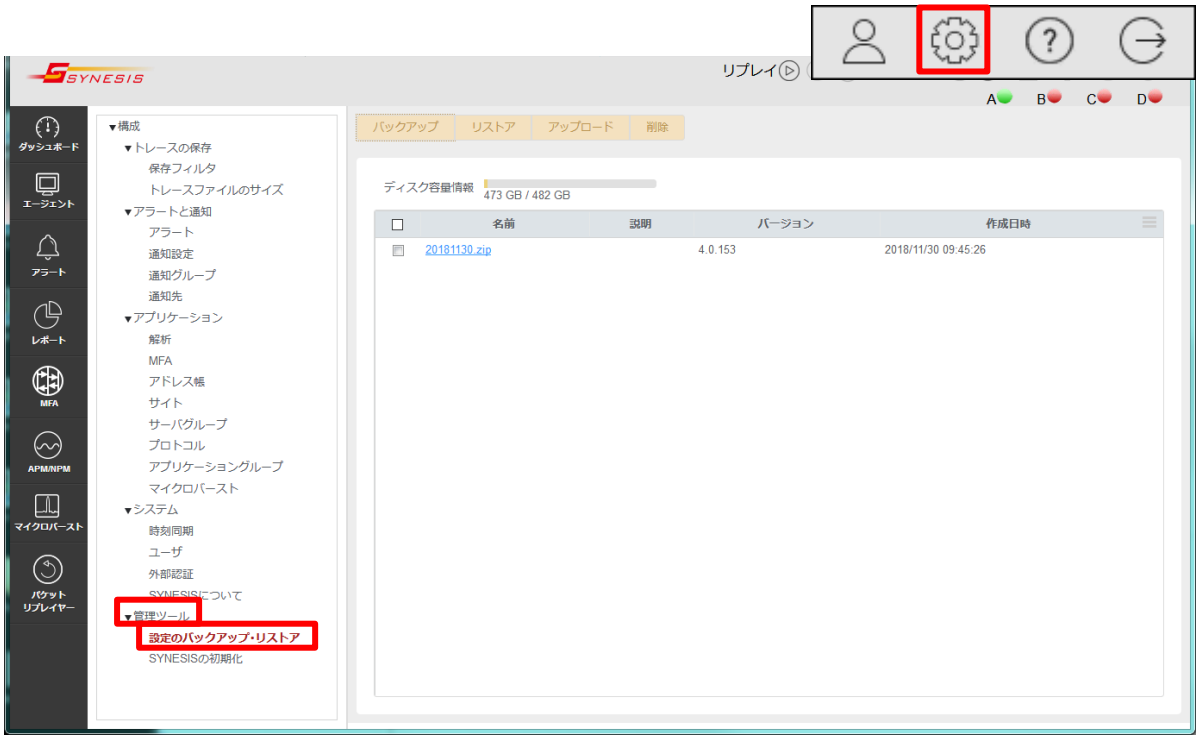
SYNESIS の構成（コンフィグ）情報のバックアップファイルを作成することができます。

保存される項目など、詳細はユーザーガイド「11-19-1. 設定のバックアップ作成とダウンロード」をご参照ください。

コンフィグ・ファイルのバックアップ作成手順は以下の通りです。

1) SYNESIS にサインインします。 ※「3.3.1.1 サインイン」参照

2) トップ画面の右側上部にある構成アイコンをクリックします。



3) [**構成**] メニュー画面が表示されます。

左側のメニューから [**管理ツール**] - [**設定のバックアップ・リストア**] を選択してください。

3)　<**バックアップ**>ボタンをクリックしてください。

4)　[**バックアップ**] 画面が表示されます。

管理者権限を持った OS のユーザ名とパスワードを入力し、ファイル名を指定してください。

5)　入力後、<**適用**>ボタンをクリックしてください。

設定情報が収められたバックアップファイルが作成され、リストに追加されます。

6)　追加されたバックアップファイルの [**名前**] 欄のリンク部分をクリックしてください。

[**バックアップファイルの編集・ダウンロード**] 画面が表示され、 バックアップファイルをダウンロードすることができます。

7.3. キャプチャ・データのバックアップ

キャプチャ・データは直接バックアップすることができません。

キャプチャ・データをバックアップしたい場合は、キャプチャ・データをトレースファイルに保存し直し、 その後、そのトレースファイルのバックアップを行ってください。

なお、キャプチャ・データがパケットストア(キャプチャ・データ保存領域)容量を超えた場合、 キャプチャ・データは古いものから順に、新しくキャプチャしたデータで上書きされて行きます。

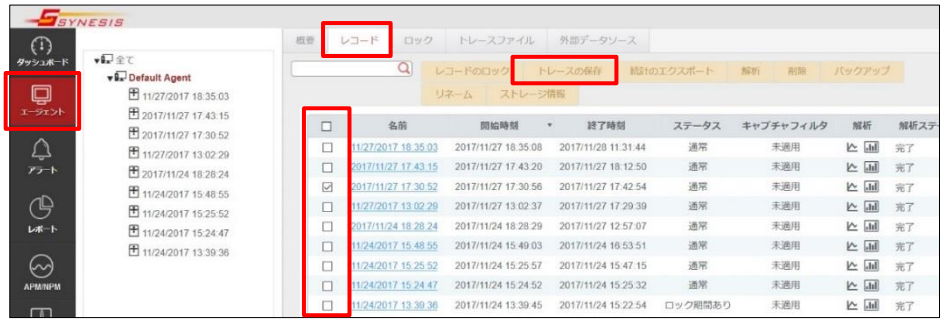
上書きされたデータは、トレースファイル化できませんのでご注意ください。

キャプチャ・データをトレースファイルに保存し直す手順は以下の通りです。

1) SYNESIS にサインインします。 ※「3.3.1.1 サインイン」参照

2) 左側のメニューから [**エージェント**] を選択し、[**レコード**] タブを選択します

3) トレースファイル化したいキャプチャ・データを含むレコードの左端のチェック欄にチェックを入れ、<**トレースの保存**> ボタンをクリックしてください。



4) キャプチャ・データの中でトレースファイル化したい期間を指定してください。
※保存期間の指定方法の詳細はユーザーガイドをご参照ください。

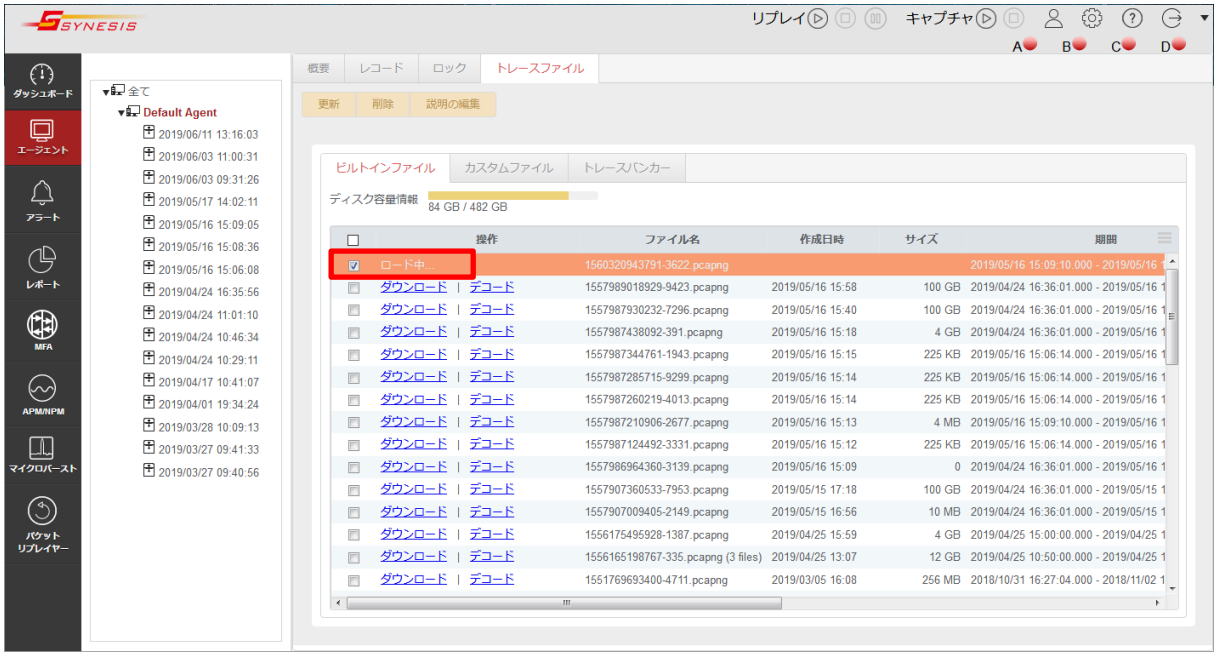
5) [**最大ファイル数**] 欄に [**0** (ゼロ)] を入力してください。 保存ファイル数の上限がなくなり、指定した期間内のデータが全てトレースファイル化されます。

6) 設定画面右下の <**トレースの保存**> ボタンをクリックしてください。

7) 自動的に [**トレースファイル**] タブが選択された状態に切り替わります。

[**操作**] 欄の表示が [**ロード中…**] から [**ダウンロード/デコード**] に変わるのを待ってください。

表示が [**ダウンロード/デコード**] に変わったら、トレースファイル化は完了です。



8) [**ダウンロード**] をクリックすると、トレースファイルをダウンロードし、 バックアップとして保存することができます。

バックアップしたトレースファイルのリストア方法は「8.3.トレース・ファイルのリストア」をご参照ください。

7.4. トレースファイルのバックアップ

トレースファイルのバックアップ手順は以下の通りです。

1) SYNESIS にサインインします。 ※「3.3.1.1 サインイン」参照

2) 左側のメイン・メニューから [**エージェント**] を選択し、[**トレースファイル**] タブを選択します。

SYNESIS 内に保存されているトレースファイルの一覧が表示されます。

3) [**操作**] 欄の [**ダウンロード可**] をクリックして、トレースファイルをダウンロードします。

4) ダウンロードされたトレースファイルをバックアップしておきます。

7.5. 作成されたレポートのバックアップ

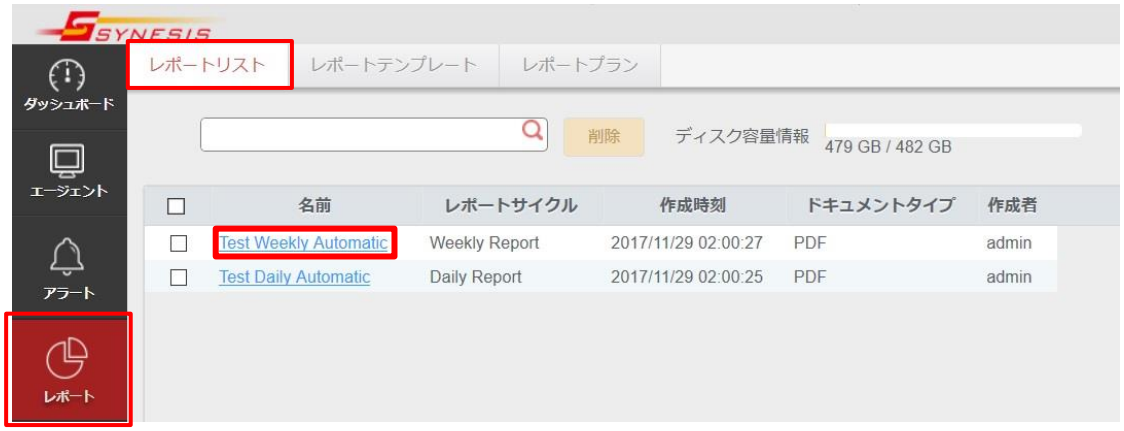
レポートメニューで作成されたレポートを pdf ファイルにして、バックアップ(保存)することが可能です。

レポートの作成に利用されるレポート・テンプレートやレポート・プランはコンフィグ・ファイルのバックアップ項目に含まれます。(※コンフィグ・ファイルのバックアップ手順は「**7.2.2. コンフィグ・ファイルのバックアップ**」をご参照ください。)

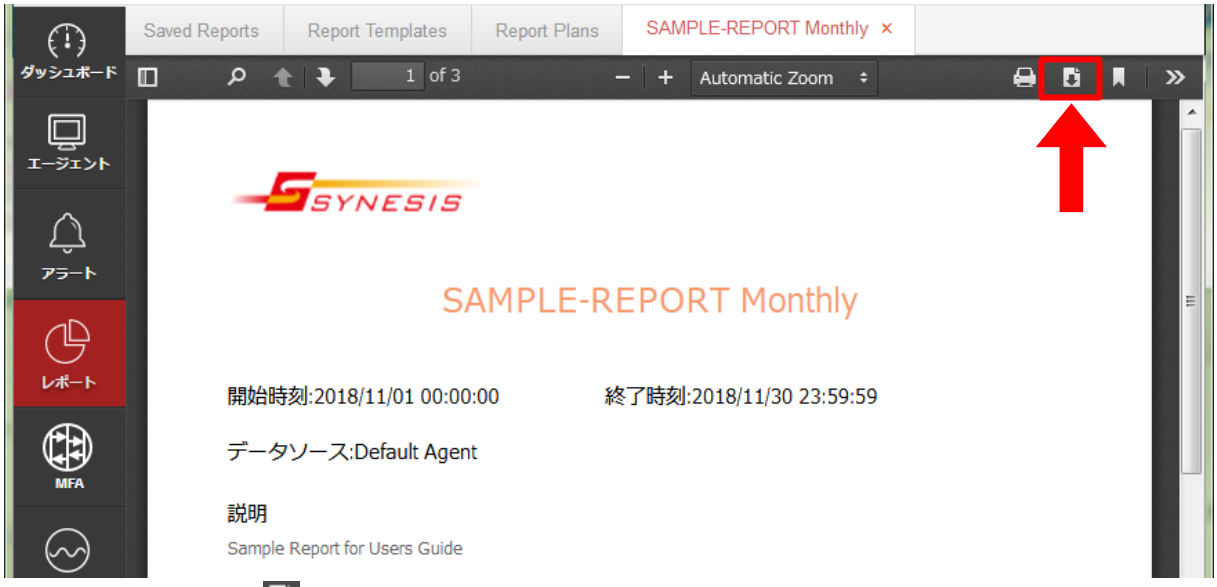
作成されたレポートのバックアップ手順は以下の通りです。

1) SYNESIS にサインインします。 ※「**3.3.1.1 サインイン**」参照

2) 左端のメイン・メニューから [**レポート**] を選択し、[**レポートリスト**] タブを選択してください。
レポート機能により作成されたレポートの一覧が表示されます。



3) 一覧からバックアップしたいレポートを選んで、名前のリンク部分をクリックしてください。
Pdf 形式のレポートが表示されます。



4) ダウンロードボタン をクリックして、レポートをバックアップ(保存)します。

8.設定情報やデータのリストア

リカバリ前に作成したバックアップファイルを使って、リカバリ後にSYNESISの設定やデータを復元(リストア)することが可能です。

バックアップを使ってリストアできるのは OS の設定情報や SYNESIS の環境・設定情報、 トレースファイルです。 それぞれの作業手順の詳細は、リンク先をご参照ください。

SYNESIS のリカバリ方法については「SYNESIS リカバリ手順書」をご参照ください。

8.1. OS 設定情報のリストア

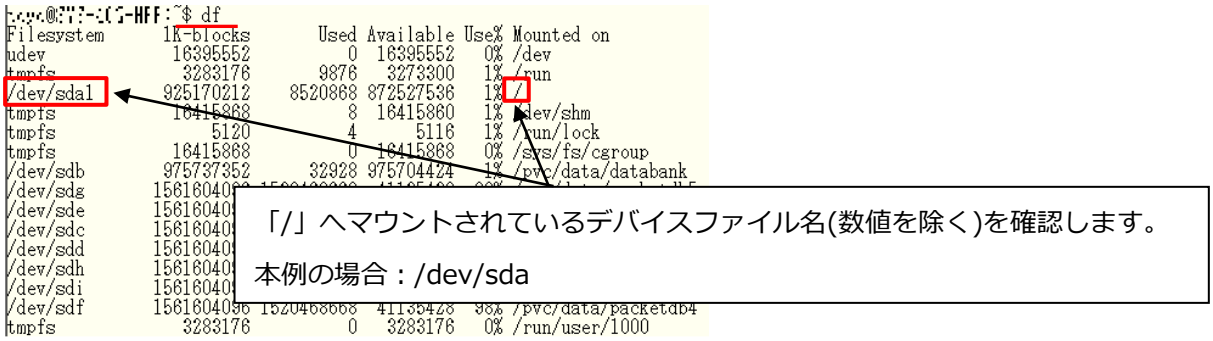
「」の手順に従って作成されたシステムイメージを、 OS がインストールされているディスク(デバイスファイル名：/dev/sda, /dev/sdb など)にリストアします。 OS がインストールされているディスクは df コマンド等で確認します。

手順は以下の通りです。

1) SYNESIS へ SSH で接続します。 ※「3.2.2 SSH」参照

2) 以下のコマンドで、OS がインストールされているディスク(デバイスファイル名)を確認します。

コマンド：df



3) 手順２）で確認できたディスクに、「**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。**」の手順に従って作成されたシステムイメージをリストアしてください。

8.2. SYNESIS 環境・設定情報のリストア

リカバリ前、バックアップを取ったライセンス・ファイルやコンフィグ・ファイルを使って、SYNESIS を元の設定に戻すことが可能です。

なお、マザー・ボードの故障などにより eth ポートの MAC アドレスが変更された場合は、 バックアップしたライセンスは利用できません。ライセンスの再発行が必要となります。

8.2.1. ライセンス・ファイルのリストア

「SYNESIS リカバリ手順書」の手順に従ってリカバリを実施し、ライセンス・ファイルのリストアが完了している場合は 本手順の実施は不要です。

次項「**8.2.2. コンフィグ・ファイルのリストア**」の手順へ移ってください。

1) リモート操作の場合は下記のアドレスを Web ブラウザのアドレスバーに入力してください。
   https://⟨*SYNESIS の IP アドレス*⟩/
2) サインイン画面が表示された場合は、本手順の実行は不要です。
   そのままサインインし、「**コンフィグ・ファイルのリストア**」を実行してください。
   下図のような「デバイス ID」が表示された場合は、手順 3)を実行してください。

3) SYNESIS へ SSH で接続します。 ※「3.3.2. SSH」参照
4) SCP などを利用して、で 保存しておいたライセンス・ファイル(pvclicense.lic)を SYNESIS へコピー/転送してください。
5) 以下のコマンド例を参考に、手順 4)で転送したファイルが保存されているディレクトリへ移動します。

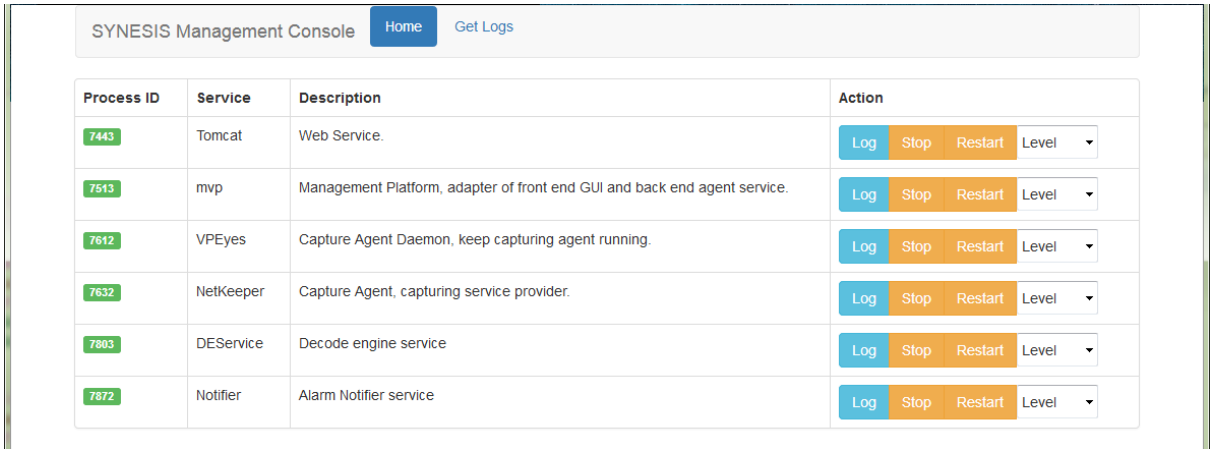
   コマンド：`cd /home/synesis/`

6) 以下のコマンドを入力し、所定の場所へライセンス・ファイルを移動します。

   コマンド：`mv pvclicense.lic /var/lib/tomcat7/`

7) ブラウザで下記の URL へアクセスします。
   https://⟨*SYNESIS の IP アドレス*⟩/mgmt/
8) ユーザ名とパスワードを入力します。
   ユーザー名(デフォルト)：admin
   パスワード(デフォルト)：synesis1

9)　以下の画面が表示されるので、Service **[Tomcat]**の**[Restart]**をクリックしてください。



10) ブラウザで下記の URL にアクセスし、サインイン画面が表示されることを確認してください。

https://⟨*SYNESIS の IP アドレス*⟩/

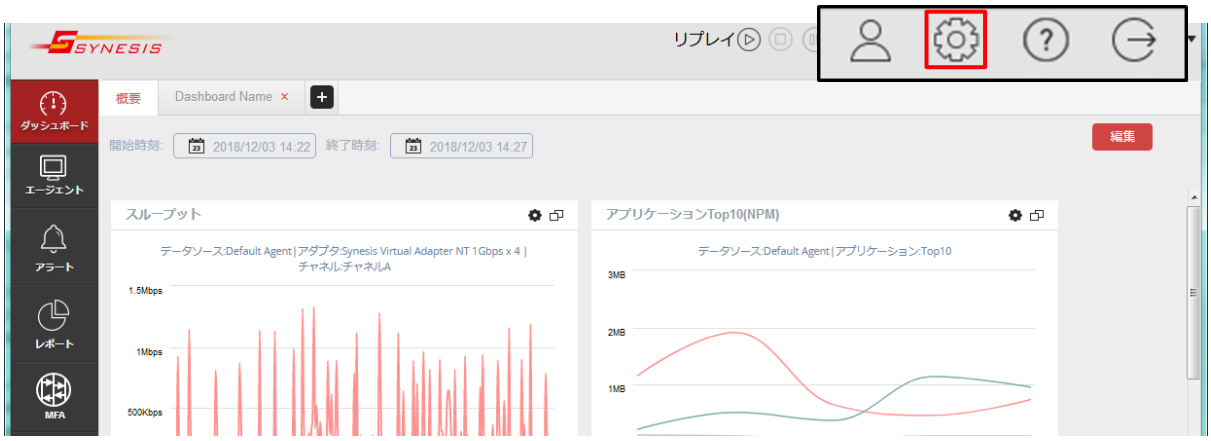
8.2.2. コンフィグ・ファイルのリストア

「7.2.2 コンフィグ・ファイルのバックアップ」の手順に従って作成されたバックアップを使って、SYNESIS を元の設定に戻すことが可能です。

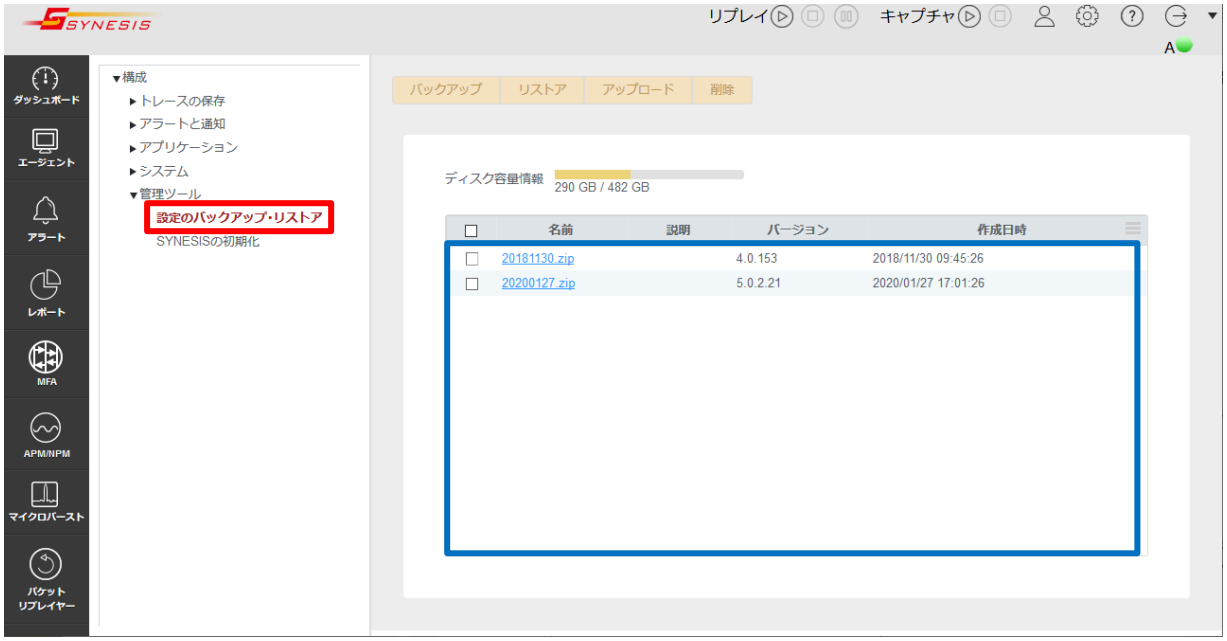
バックアップで保存される項目についてはユーザーガイドをご参照ください。

1)　SYNESIS にサインインします。　※「3.3.1.1 サインイン」参照

2)　トップ画面の右側上部にある構成アイコンをクリックします。



3) [**構成**]メニュー画面が表示されます。左側のリストから **[管理ツール]** → **[設定のバックアップ・リストア]** を選択してください。



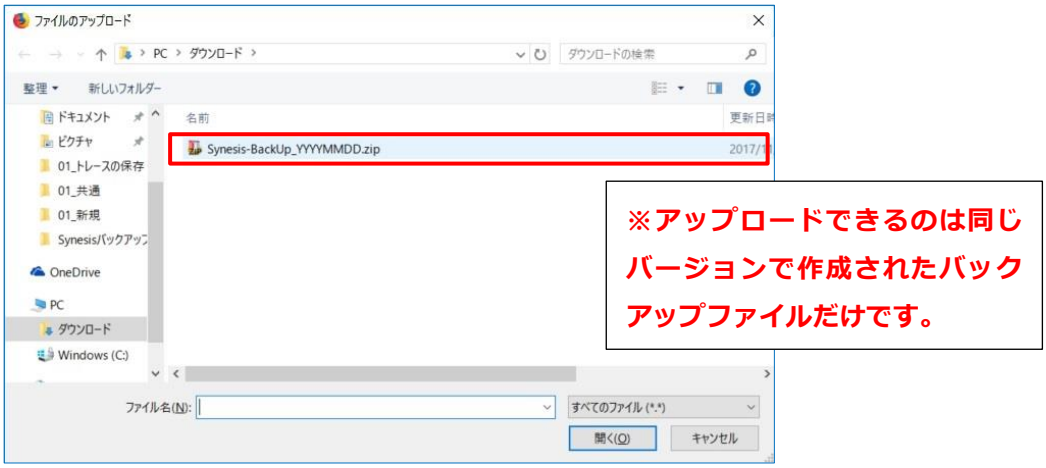
4) [**設定のバックアップ・リストア**] 画面が表示されましたら、復元（リストア）したいバックアップファイルが一覧(上図青枠)内にあるか確認してください。

5) リストア対象となるバックアップファイルがある場合は、ファイル名の左側にあるチェックボックスにチェックを入れて<**リストア**>ボタンをクリックし、手順 10) へ進んでください。
リストア対象となるバックアップファイルが一覧にない場合は、手順 6)に進んでください。

6) [**設定のバックアップ・リストア**] 画面の上部の<**アップロード**>ボタンをクリックしてください。

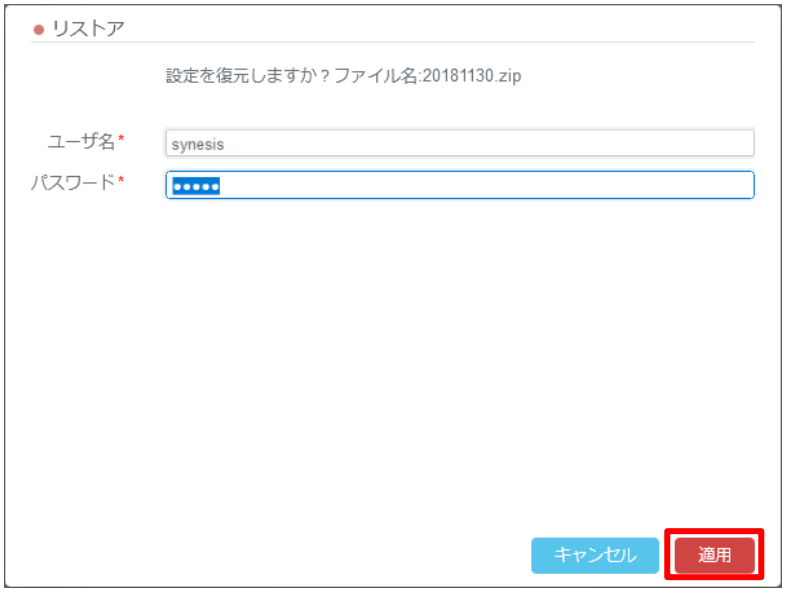
7) 以下の画面が表示されるので、**<参照>**ボタンをクリックしてください。

8) **[ファイルのアップロード]** 画面よりアップロードするファイルを選択してください。

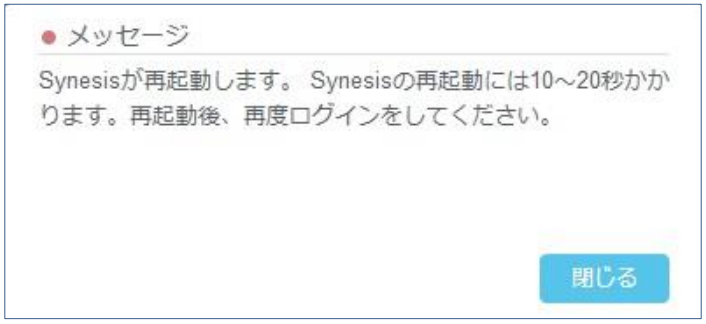


9) アップロードするファイルを選択して**<開く>**ボタンをクリックすると、[アップロード] 画面にバックアップファイルの情報が表示されます。情報を確認し問題なければ<**アップロード**>ボタンをクリックしてください。

10) 以下のパスワード入力画面が表示されます。管理者権限を持つ OS のユーザ名とパスワードを入力して＜**適用**＞ボタンをクリックしてください。

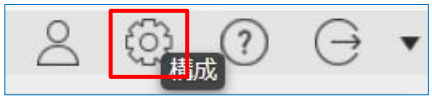


11) リストア完了後、以下のポップアップ画面が表示されますので、確認後＜**閉じる**＞ボタンをクリックしてください。



12) SYNESIS へ再度アクセスし、サインインします。

13) 構成アイコンをクリックし、コンフィグ(設定)情報が反映されていることを確認してください。



8.3. トレース・ファイルのリストア

バックアップされたトレース・ファイルは、SYNESIS の「トレースバンカー」機能で読み込めます。 また、Wireshark などの pcap ファイル参照・解析ツールで参照することも可能です。

トレース・ファイルを SYNESIS 外部の保存先から読み込む手順は以下の通りです。

1) SYNESIS にサインインします。 ※「3.3.1.1 サインイン」参照

2) メインメニューから[**エージェント**] を選択し、[**トレースバンカー**]タブをクリックしてください。
外部からトレース・ファイルを読み込ませることが可能な [**トレースバンカー**] 画面が表示されます。

3) **<アップロード>**ボタンをクリックしてください。
以下の**[アップロード]**ダイアログが表示されます。

4) **<参照>**ボタンをクリックし、読み込むファイルを指定してください。

5) <**トレースファイルをアップロード**>ボタンをクリックしてください。
指定したファイルがアップロードされ、一覧に追加されます。

8.4. レポート設定のリストア

レポートの作成に利用されるレポート・テンプレートやレポート・プランは コンフィグ・ファイルのバックアップ項目に含まれており、 コンフィグ情報のバックアップを使って、同じ形式のレポートを作成することが可能です。詳細はユーザーガイドの「5. レポート」をご参照ください。

なお、バックアップとして pdf ファイルで保存したレポートを復元(リストア)・参照することはできません。pdf ファイルビューワーなどで参照してください。

9.簡易動作確認手順

本章では、SYNESIS の電源投入後の動作確認として実行できる、簡易動作確認手順について説明します。障害・異常発生時の問題個所確認としてもご利用いただけます。

9.1. キャプチャポートのリンクステータス確認

スイッチやタップなど、トラフィックをキャプチャしたい SYNESIS の対向側のポートと、SYNESIS のキャプチャポートがリンクしているかどうか、リンクステータスを確認します。SYNESIS のキャプチャポートと対向側のポートを接続した上で、以下の項目を確認してください。

① 対向側のポートがトラフィックを流す設定・構成になっていること

② 対向側のポートと、SYNESIS のキャプチャポート※が接続されていること

③ 項目②で確認した SYNESIS キャプチャポートのリンク LED が「**点滅**」していること

「消灯」の場合、SYNESIS の対向とリンクしていません。

「点灯」の場合、SYNESIS の対向とリンクしていますが、トラフィックが流れてきていません。

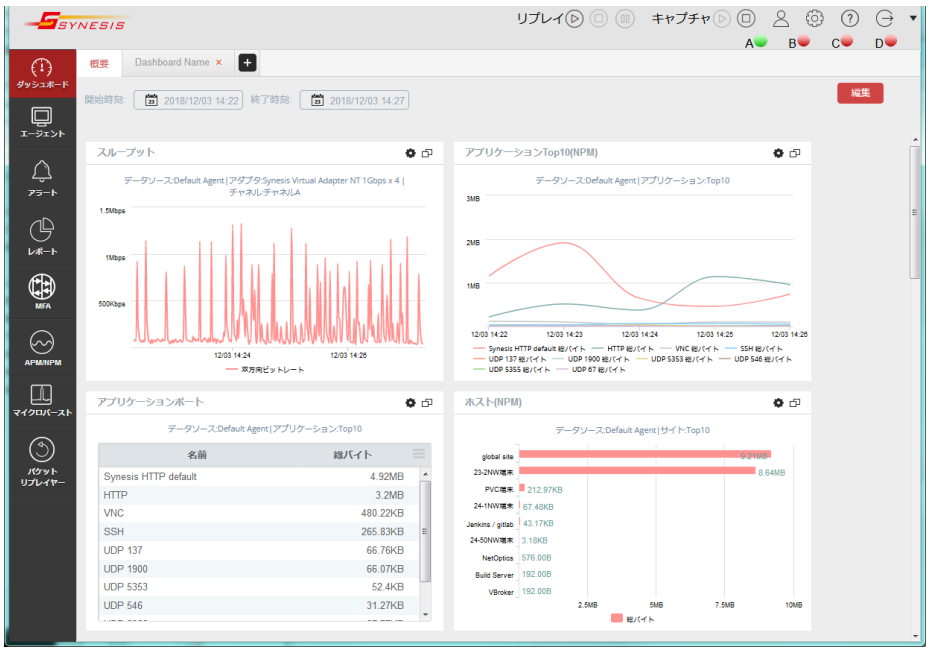
※SYNESIS のポートの位置は**[構成 ⚙] - [SYNESIS について]**よりご確認いただけます。

9.2. SYNESIS へのアクセス

SYNESIS の電源を投入したら、正常に SYNESIS にアクセスできるかを確認してください。手順は以下の通りです。

1) SYNESIS にサインインします。 ※「3.3.1.1 サインイン」参照

2) サインイン後、SYNESIS の [**ダッシュボード**] 画面が表示されることをご確認ください。



9.3.キャプチャの動作確認

起動した SYNESIS にアクセスできましたら、 SYNESIS の設定を確認した上でキャプチャを開始し、キャプチャが正常に行われることを確認してください。

9.3.1. SYNESIS の設定の確認

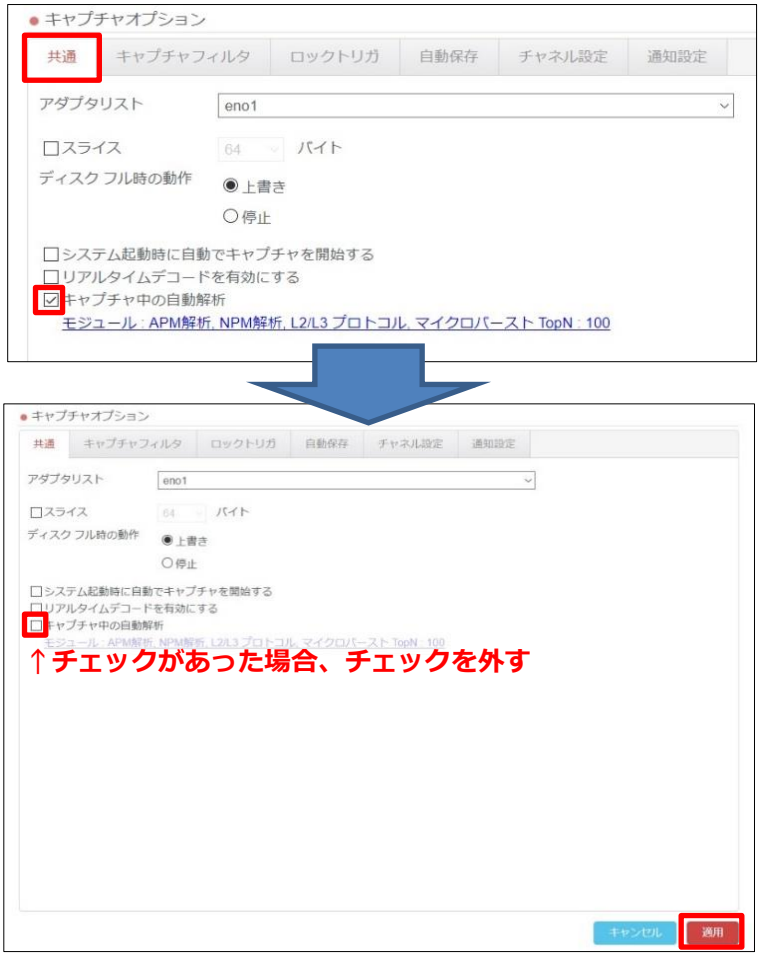
キャプチャを開始する前に、SYNESIS の設定を確認してください。確認の手順は以下の通りです。

1) ツールバー上のリンクステータスの表示が [●] になっていることを確認してください。

2) 画面左側のメニューから [**エージェント**] を選択し、[**概要**] タブ内の <**オプション**> ボタンをクリックします。

3) [**キャプチャオプション**] 画面の [**共通**] タブを表示させ、[**キャプチャ中の自動解析**] にチェックがないことを確認します。

※チェックがあった場合、チェックを外してください。



4) <**適用**>ボタンをクリックしてください。（すでにキャプチャ中の場合は、<適用>ボタンは無効になっています。）

9.3.2. キャプチャの開始

1) 画面左側のメニューから [**エージェント**] を選択してください。

2) キャプチャのステータスが "停止" の場合は、 <**キャプチャの開始**> ボタンをクリックします。
キャプチャのステータスが "キャプチャ" の場合は、そのまま次の手順に移ってください。

3) キャプチャのステータスが "キャプチャ" に変わることを確認してください。v

9.3.3. キャプチャ開始後の確認項目

キャプチャを開始後、 1～2 分待ってから、画面内の以下項目を確認してください。

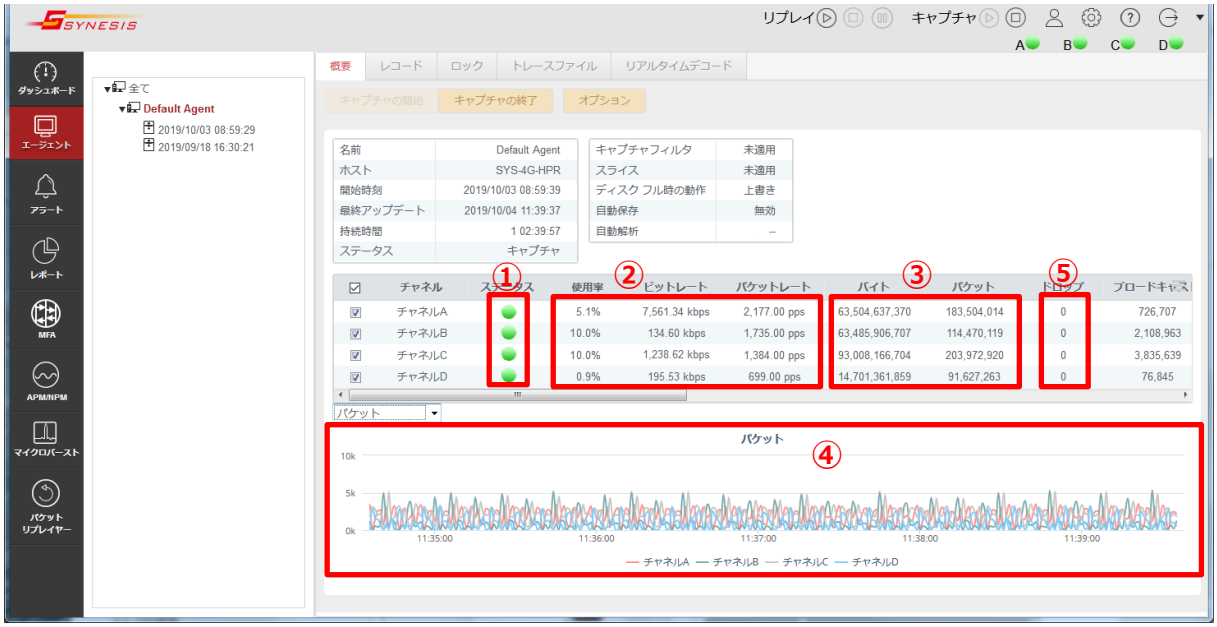
① トラフィックが流れているポート(チャネル)のステータスが "緑●" になっていること

② トラフィックが流れているポート(チャネル)の "使用率"、"ビットレート"、"パケットレート" に "0(ゼロ)" 以外の数値が表示されていること

③ トラフィックが流れているポート(チャネル)の "パケット"と"バイト"のカウントが増加すること

④ キャプチャを開始後、データがグラフにプロットされていること

⑤ "ドロップ" が "0(ゼロ)" であること



9.4. iDRAC のステータス確認

iDRAC により、SYNESIS のハードウェアのステータスを確認することができます。

9.4.1. iDRAC8

1) iDRAC にログインします。 ※「3.4.1.1 ログイン」参照

2) 左側のメニューから [**概要**] - [**サーバー**] を選択します。

3) 以下の [**システム概要**] 画面が表示されます。

[**サーバーの正常性**] 欄のチェックがすべて緑色であることを確認してください。

4) 左側のメニューから [**概要**] → [**ストレージ**] を選択します。

5) 以下の [**ストレージ概要**] 画面が表示されます。

[**物理ディスクの概要**] 欄の円グラフがすべて緑色（オンライン）であることを確認してください。

以上で簡易動作確認は完了です。ブラウザを閉じて構いません。

9.4.2. iDRAC9

1) iDRAC にログインします。 ※「3.4.2.1 ログイン」参照

2) 以下のダッシュボード画面が表示されます。

画面左上の [**正常性情報**] の欄のチェックがすべて緑色であることを確認してください。

以上で簡易動作確認は完了です。ブラウザを閉じて構いません。

10. 障害・異常発生時の対応手順

SYNESISで障害と思われる事象が発生した場合は、弊社のSYNESISサポートグループまでお問い合わせ願います。お問い合わせの際には、以下の情報をご連絡ください。

- **発生した事象のまとめ**
- **簡易動作確認の実施と結果の確認**
- SYNESISのログ

10.1. 発生した事象のまとめ

障害と思われる事象に関する情報(SNMP Trap, Syslog, LEDの内容、等)の収集をお願いします。

- 通常青色で点灯のHW LEDがオレンジ色で点滅している
- iDRACからSNMP Trapを受信した
- SYNESISを操作できない

10.2. 簡易動作確認の実施と結果の確認

障害と思われる事象が発生した場合には、「**9. 簡易動作確認手順**」に従って簡易動作確認を実施してください。

確認の結果、問題があった場合は、問題があった箇所の画面キャプチャを取得してください。

※画面キャプチャが取得できない場合、下記の情報をご提供ください。

□ SYNESIS のポートごとのステータスが「緑」になっているか。

□ SYNESIS の各統計値がキャプチャ中に更新されているか。

□ SYNESIS の「ドロップ」欄のカウントが 0 であるか。

□ iDRAC ポートの「サーバの正常性」欄が、全て緑のチェックとなっているか。

□ iDRAC ポートの「物理ディスクの概要」欄が、全てオンラインとなっているか。

10.3. ログの取得

「**11. ログの取得**」に従い、ログの取得をお願いします。

10.4. お問い合わせ

お問い合わせ内容と共に「10.1～10.3 にて確認・取得した情報」を下記弊社サポート宛てへお送りください。

[問い合わせ先]

株式会社東陽テクニカ

技術部 SYNESIS サポートグループ

TEL：03-3279-0771(代表)　03-3245-1107(直通)

FAX：03-3246-0645

E-Mail　：synesis-support@toyo.co.jp

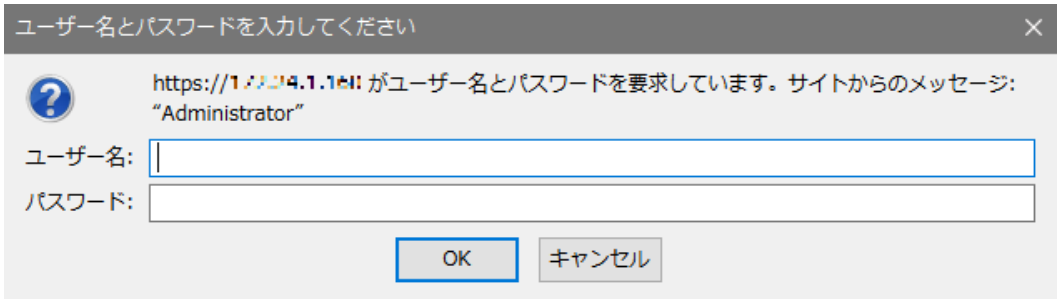
受付時間：月曜～金曜 9:30~17:30 (土日、祝日、年末年始および弊社指定休日を除く)

11. ログの取得

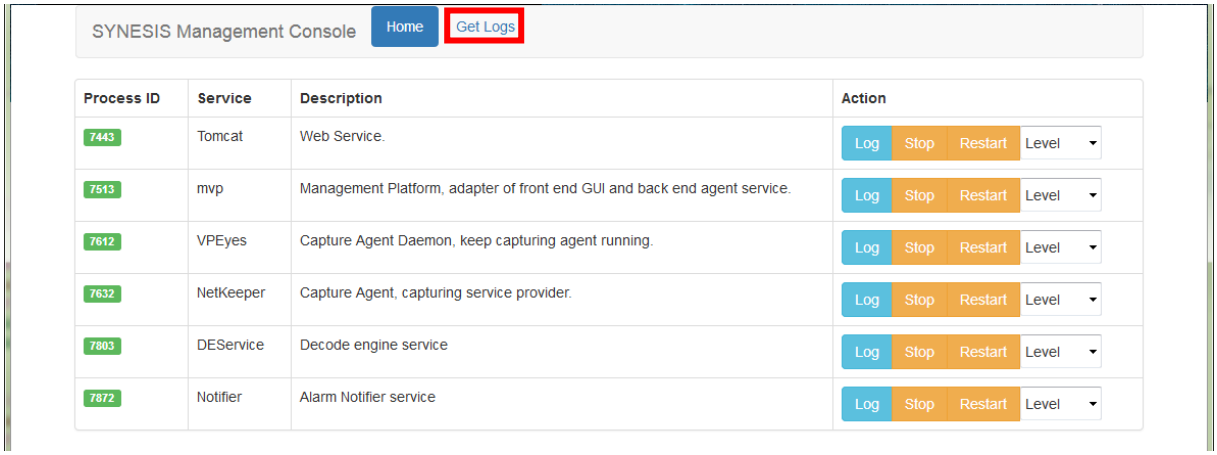
SYNESIS のログ取得手順について説明します。

1) 下記のアドレスを Web ブラウザ(FireFox)のアドレスバーに入力してください。
https://（*管理ポートの IP アドレス*）/mgmt/

2) 以下の画面が表示されるので、管理者権限を持った SYNESIS アカウントのユーザ名、パスワードを入力して、 **<OK>**ボタンをクリックしてください。
※「3.3.2. サービス・ログ管理 GUI」の「3.3.2.1 ログイン」参照



3) 以下のサービス・ログ管理画面が表示されます。**[Get Logs]**をクリックしてください。



4) 以下のダイアログが表示されるので、ログを保存してください。

東陽テクニカ
Synesis 管理者マニュアル

Copyright © 2017-2018 TOYO Corporation All Rights