

さくらのクラウド「Sophos UTM」

Owlook

サービス利用手順書

かんたん初期導入編

第 1.1 版

2018 年 6 月 29 日



興安計装株式会社

目次

内容

改訂履歴.....	2
はじめに.....	3
1. サービスについて.....	4
(1) サービス提供内容.....	4
(2) サービス提供範囲.....	4
(3) サービス利用条件.....	6
①ご利用環境.....	6
②推奨導入構成.....	6
③サイジング.....	7
(4) サービス利用の流れ.....	7
(5) サービス提供範囲外の機能について.....	8
2. ご利用環境の構成.....	9
3. Sophos UTM9 の初期展開.....	10
(1) 共有セグメントへの展開.....	10
(2) IP アドレスの手動割り当て.....	15
(3) ライセンスサーバに接続する手順.....	23
(4) サービス終了手順.....	26
4. 初期設定.....	28
4-1. Sophos UTM9 の初期設定.....	28
(1) UTM の基本情報変更手順.....	28
(2) 管理者パスワード変更手順.....	29
(3) Shell アクセス (SSH) のパスワード変更手順.....	30
(4) Syslog 連携手順.....	31
(5) NIC を追加し IP アドレスを割り当て手順.....	34
(6) マニュアル参照手順.....	41
(7) バックアップ取得手順.....	43
(8) リストア手順.....	44
4-2. 保護対象システム (WindowsServer2012R2) の初期設定.....	47

改訂履歴

版数	更新日	更新内容	更新者
1.0	2018/1/25	初版作成	興安計装株式会社
1.1	2018/6/29	US キーボード配列の仕様を補足説明として追加。	興安計装株式会社

はじめに

本手順書に関する注意事項

この手順書は、一般的な評価環境を簡単なステップで構築するための補助資料です。導入に際して必要な全てのトピックについての網羅的な解説は意図しておりません。個々のトピックについての詳細は、管理者ガイドをご確認頂くようお願い致します。

本サービスにおけるお問い合わせは、さくらインターネット株式会社が提供するサポート窓口をご利用いただくか、技術情報にて公開されたナレッジをご参照ください。本サービスの製品 SophosUTM9 の開発元であるソフォス株式会社への直接の問い合わせを固く禁じます。

本手順書の目的と位置づけ

目的:保護対象システム（サーバ若しくはクライアント）を Sophos UTM9 の配下に展開するまでの初期設定手順をご提供すること。

本手順書を順番に沿って設定を進めて頂くことにより、Sophos UTM9 によるシステムの保護に必要な初期構成が可能となります。サブスクリプションにより利用可能となる各種プロテクションの手順については、本手順書には記載しておりません。

1. サービスについて

(1) サービス提供内容

提供項目	内容
Sophos UTM9 アーカイブイメージ	一部機能を除き、動作検証及び初期設定が完了した状態のアーカイブイメージを提供します。
Sophos UTM9 利用ライセンス	当社が提供したアーカイブイメージから展開したSophosUTM9 のみが適用可能なライセンスを提供します。

(2) サービス提供範囲

本サービスで提供される SophosUTM9 の機能は以下の通りです。

サービス項目	機能
ネットワークサービス	・ DNS ・ DHCP ・ NTP 上記に付随する各種オプション
ユーザポータル	リモートアクセスサービスを提供するブラウザベースアプリケーションと付随する各種オプション
ネットワークプロテクション	・ ファイアウォール ・ 侵入防御(IPS) ・ 高度な防御機能(ATP) 上記に付随する各種オプション
Web プロテクション	・ Web フィルタリング ・ アプリケーションコントロール 上記に付随する各種オプション
Eメールプロテクション	・ SMTP プロキシ ・ POP3 プロキシ 上記に付随する各種オプション
高度な防御	よりリスクの高い通信の防御
Web サーバプロテクション	・ Web Application Firewall (WAF) 上記に付随する各種オプション

サイト間 VPN	<ul style="list-style-type: none">• IPsec• SSL• Amazon VPC
リモートアクセス	<ul style="list-style-type: none">• SSL• PPTP• L2TP over IPsec• IPsec• HTML5 VPN ポータル• Cisco™ VPN クライアント
ログとレポート	<ul style="list-style-type: none">• 各サービスのログ取得• 各サービスのレポート作成• エグゼクティブサマリーレポートの作成

本サービスで提供される SophosUTM9 の詳細機能については Owllook セキュリティマネジメン
トサービス仕様書内の 3. 提供機能の詳細をご参照ください。

(3) サービス利用条件

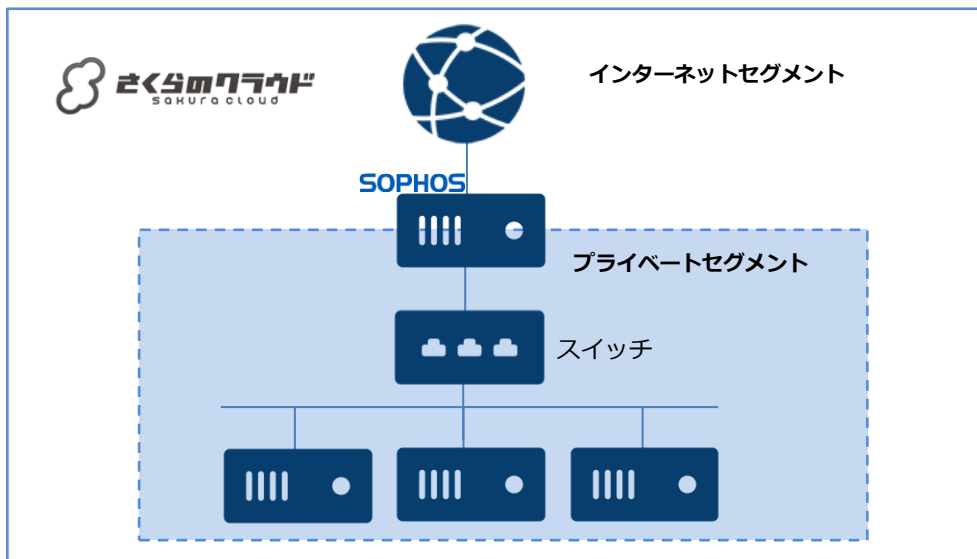
本サービスの利用条件は以下の通りです。

①ご利用環境

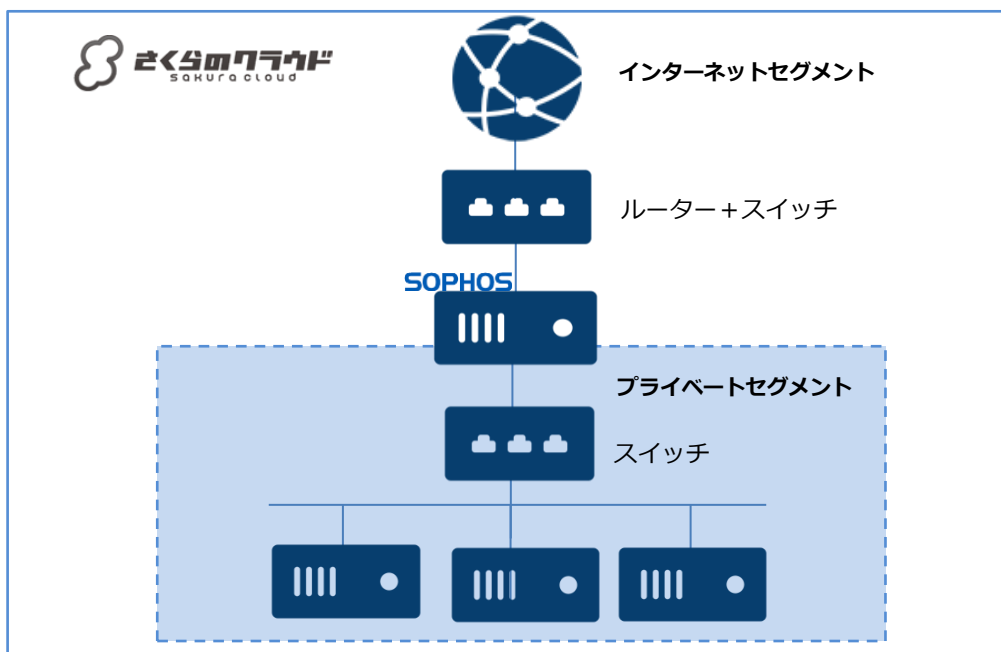
さくらのクラウドサービス内の全てのリージョンよりご利用可能です。

②推奨導入構成

Sophos UTM9 はご利用の環境における外部（インターネット）との接続点への導入し、内部はスイッチを利用しセグメントを構築してください。



また以下のように、ルーター+スイッチ機能で SophosUTM9 へ任意の IP アドレスを設定することが可能です。



③サイジング

さくらのクラウドサービス環境へ SophosUTM9 を展開した場合のスペック目安は以下の通りです。あくまで目安でありパフォーマンスを保証する数値ではありません。ハイパーバイザーのご利用環境によって最大 10%までのパフォーマンスの低下が予想されます。

vCPU	2	2	4	4	2*6	2*10
メモリ(GB)	4	8	12	16	24	48
HDD(GB)	100※1					
FW 最大※2 (Mbps)	3,100	13,000	20,000	25,000	40,000	60,000
IPS 最大 (Mbps)	750	3,000	6,000	7,000	12,000	16,000
FW + ATP + IPS 最大 (Mbps)	680	2,850	5,890	6,650	11,980	14,600
新規最大 TCP 接続/秒	24,000	70,000	120,000	130,000	160,000	190,000
同時最大 TCP 接続数	2,000,000	4,000,000	6,000,000	8,000,000	12,000,000	20,000,000
同時最大接続 IPsec VPN トンネル数	175	500	1,200	1,600	2,200	2,800
同時接続 SSL VPN トンネル数	75	200	250	280	340	420

※1 Disk サイズの推奨は 100GB です。ログの保持には Syslog サーバへの転送機能を推奨します。

※2 1518 バイトのパケットサイズ、デフォルトのルールセット環境の目安値です。

(4) サービス利用の流れ

本サービスご利用までの流れは以下の通りとなります。実施内容についての詳細手順はさくらインターネットより技術情報として公開されています。

提供ステップ	実施内容
①さくらのクラウドサービスのアカウント取得	本サービスはさくらのクラウドサービス上で提供可能なサービスとなります。その為、利用者はさくらのクラウドサービスが利用できる状態であることが前提となります。
②SophosUTM9 の展開	さくらのクラウドサービスより本サービスより提供される SophosUTM9 のアーカイブイメージをパブリックアーカイブから展開します。
③利用規約へ同意	SophosUTM9 へ初回ログイン時に表示される URL より利用規約を確認し、同意頂きます。

④ライセンスサーバーへの接続	SophosUTM9 へ当社が提供するライセンスサーバへ接続設定を行います。
⑤利用ライセンスの有効化	SophosUTM9 がライセンスサーバへ接続後、利用ライセンスが有効になります。利用ライセンスの有効化処理はご利用環境によって 30 分程お待ちいただく事があります。
⑥利用開始	SophosUTM9 の機能がご利用いただけるようになり、利用者にて設定が可能となります。
⑦利用終了	SophosUTM9 を一定期間停止、または削除した場合、ライセンスは破棄され利用終了となります。

(5) サービス提供範囲外の機能について

本サービスで提供される Sophos UTM9 利用ライセンスはほぼすべての機能をご利用いただく事が可能なライセンスです。その為、本サービス仕様書に記載のない機能も利用ライセンスに含まれます。

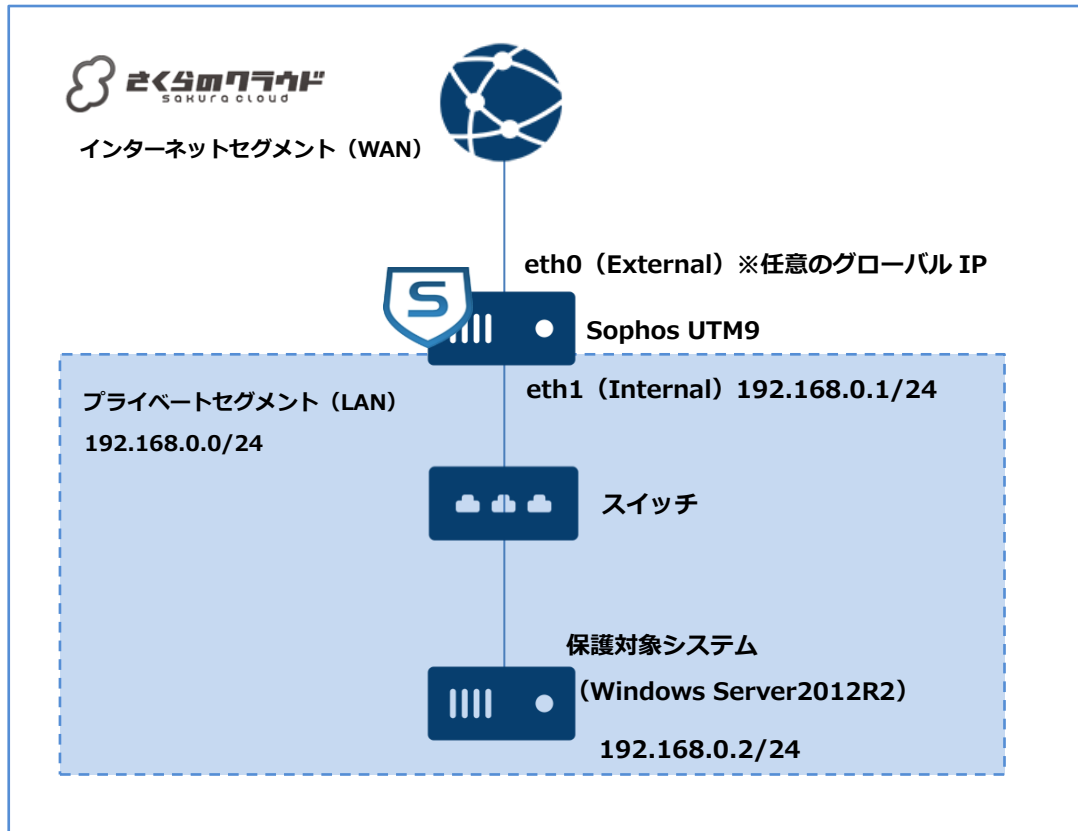
またさくらのクラウドサービス環境では、Sophos UTM9 に搭載された HA クラスタ機能及びブリッジインターフェースの構成をご利用いただく事ができません。

本サービス仕様書に記載がある機能は、推奨導入構成において動作確認ができています。

本サービス仕様書に記載のない機能または、推奨外の構成でご利用いただく場合、本サービス内でサポートすることはできません。本サービス仕様書に記載のない機能または、推奨外の構成は、利用者の責任でご利用いただきますようお願い致します。

2. ご利用環境の構成

本手順書では以下の構成であることを前提に記載いたします。



【構成要件】

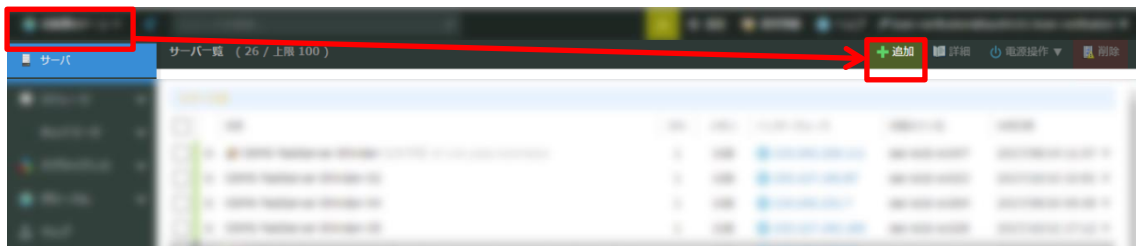
- Sophos UTM9 はご利用の環境におけるインターネットとの接続点へ導入します。
- Sophos UTM9 はインターネットセグメント (WAN) 側とプライベートセグメント (LAN) 側の 2 つの NIC を持ちます。プライベートセグメント (LAN) 側の IP アドレスは 192.168.0.1/24 を持ちます。
- プライベートセグメント (LAN) は 192.168.0.0/24 のネットワーク帯域で構成します。
- プライベートセグメント (LAN) はスイッチを利用しセグメントを構築します。
- 保護対象システムの IP アドレスは 192.168.0.2/24 を持ちます。
- 保護対象システムのデフォルトゲートウェイは Sophos UTM9 のプライベートセグメント (LAN) 側の IP アドレス 192.168.0.1/24 を向いています。

3. Sophos UTM9 の初期展開

(1) 共有セグメントへの展開

インターネット側の IP アドレスが自動的に割り当てられます。

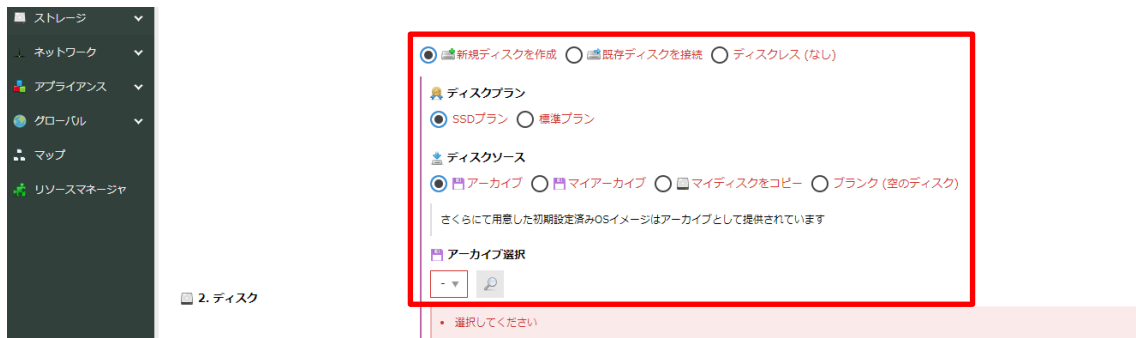
①展開先のゾーンを選択し、「追加」ボタンを押下します。



②シンプルモードのチェックを外し、適切なサーバプランを選択します。



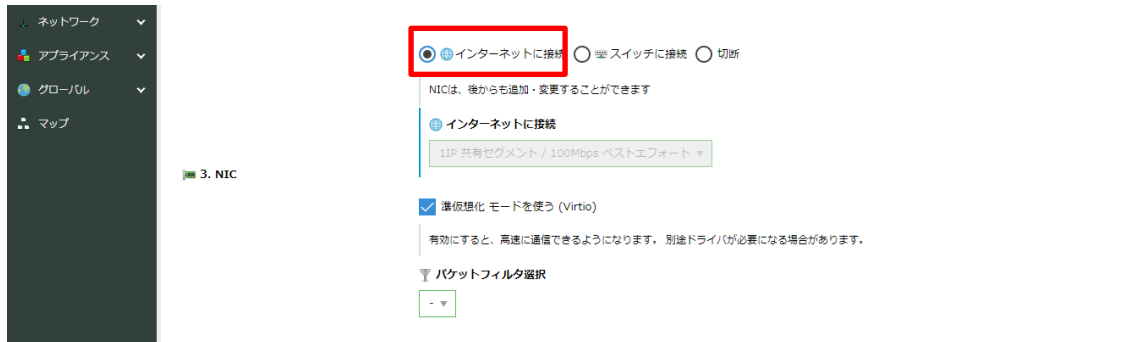
③適切なディスクプランを選択し、アーカイブから UTM のアーカイブを選択します。



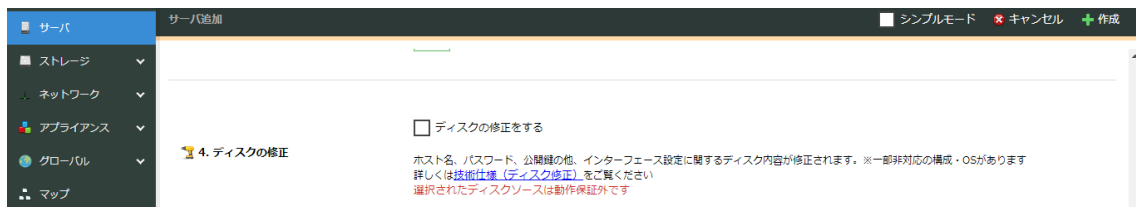
④ディスクサイズは 100GB を選択します。



⑤インターネットに接続を選択します。



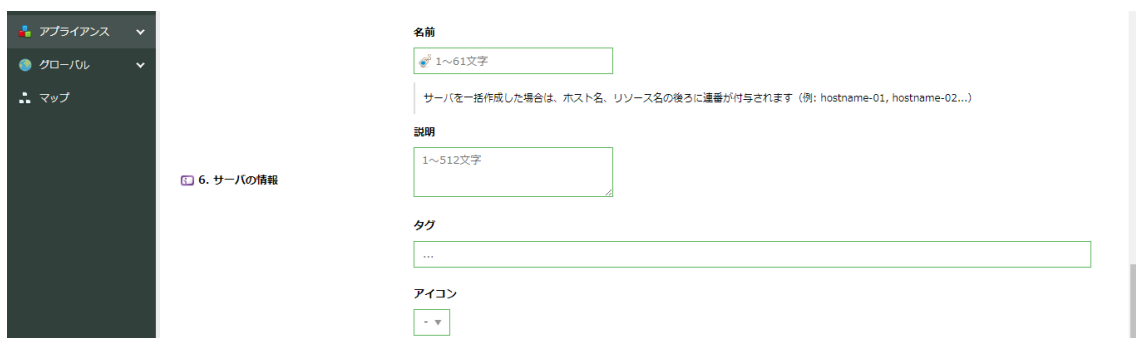
⑥UTM のアーカイブに対し、ディスク修正は利用できません。



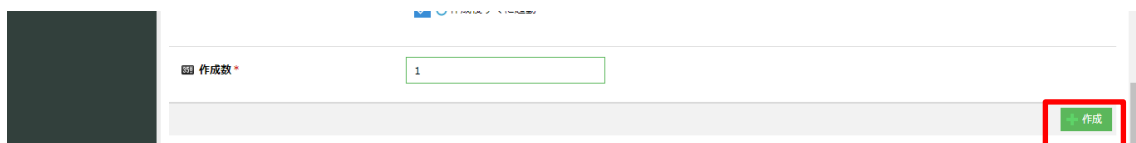
⑦シンプル監視は任意で有効にします。



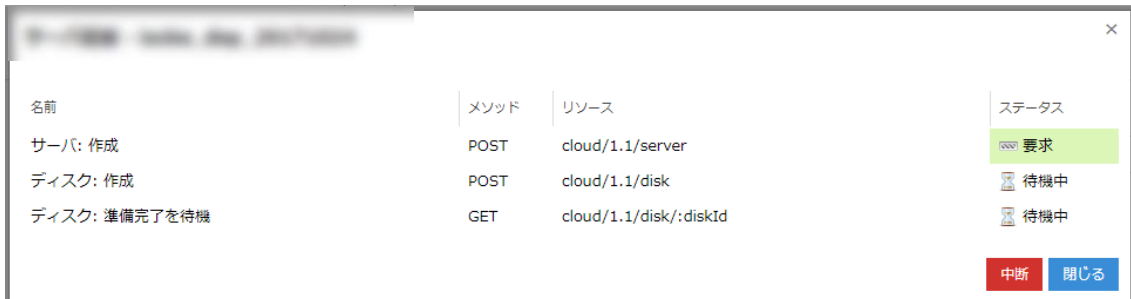
⑧サーバの情報は任意の内容で入力します。



⑨作成ボタンを押下します。



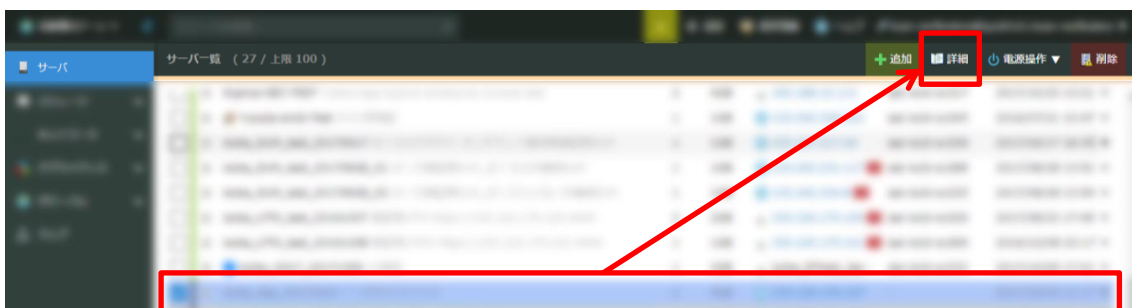
⑩サーバの追加プロセスが開始されます。



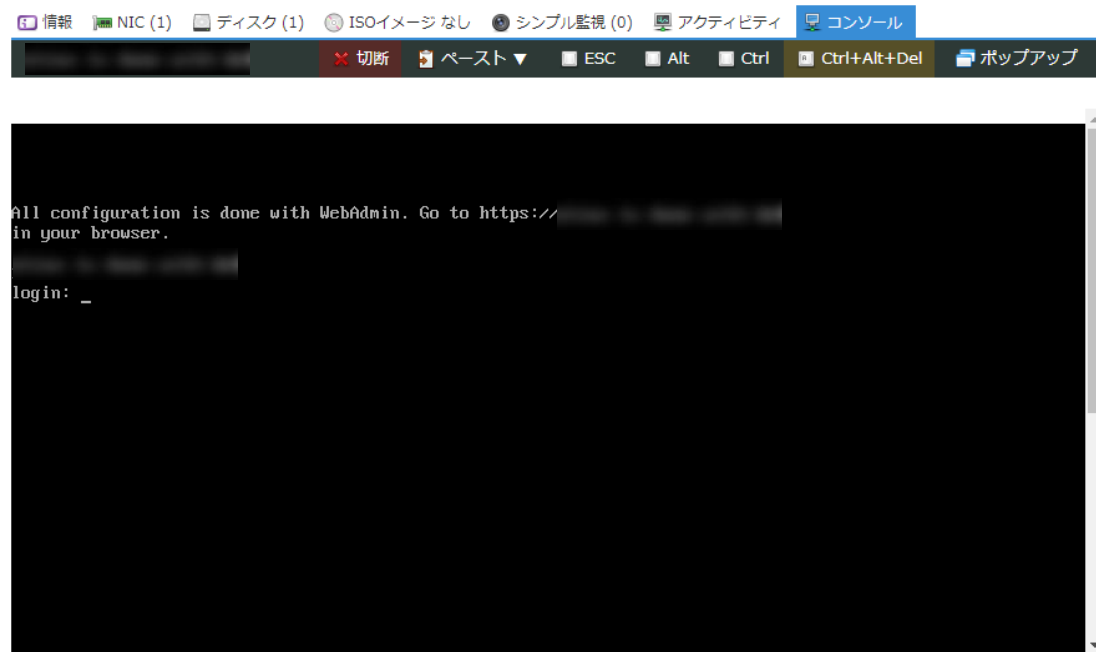
名前	メソッド	リソース	ステータス
サーバ: 作成	POST	cloud/1.1/server	要求
ディスク: 作成	POST	cloud/1.1/disk	待機中
ディスク: 準備完了を待機	GET	cloud/1.1/disk/:diskId	待機中

中断 閉じる

⑪サーバが作成されたら、作成されたサーバを選択し、詳細を押下します。



⑫コンソールを開きます。



⑬root アカウントでログインします。初期パスワードは「Ys15Vbt96L」です。

```
All configuration is done with WebAdmin. Go to https://[redacted]
in your browser.

login: root
Password:

Sophos UTM
(C) Copyright 2000-2017 Sophos Limited and others. All rights reserved.
Sophos is a registered trademark of Sophos Limited and Sophos Group.
All other product and company names mentioned are trademarks or registered
trademarks of their respective owners.

For more copyright information look at /doc/astaro-license.txt
or http://www.astaro.com/doc/astaro-license.txt

NOTE: If not explicitly approved by Sophos support, any modifications
done by root will void your support.

sophos_utm_9:/root #
```

⑭以下のコマンドを入力し Enter を押下し、戻り値が「1」であることを確認します。

ご注意：コンソールからの入力時、US キーボード配列仕様となっております。

「_」（アンダーバー）は Shift キーを押しながら以下の箇所を入力することができます。

!	@	#	\$	%	^	&	*	()	-	+	
1	2	3	4	5	6	7	8	9	0	_	=	

日本語キーボードの「ほ」の位置に該当します。

Q	W	E	R	T	Y	U	I	O	P	{	}
										[]

A	S	D	F	G	H	J	K	L	:	"	
									;	'	\

Z	X	C	V	B	N	M	<	>	?	
							,	.	/	

※US キーボード配列

```
# cc reset_system_id
```

```
All configuration is done with WebAdmin. Go to https://[redacted]
in your browser.

login: root
Password:

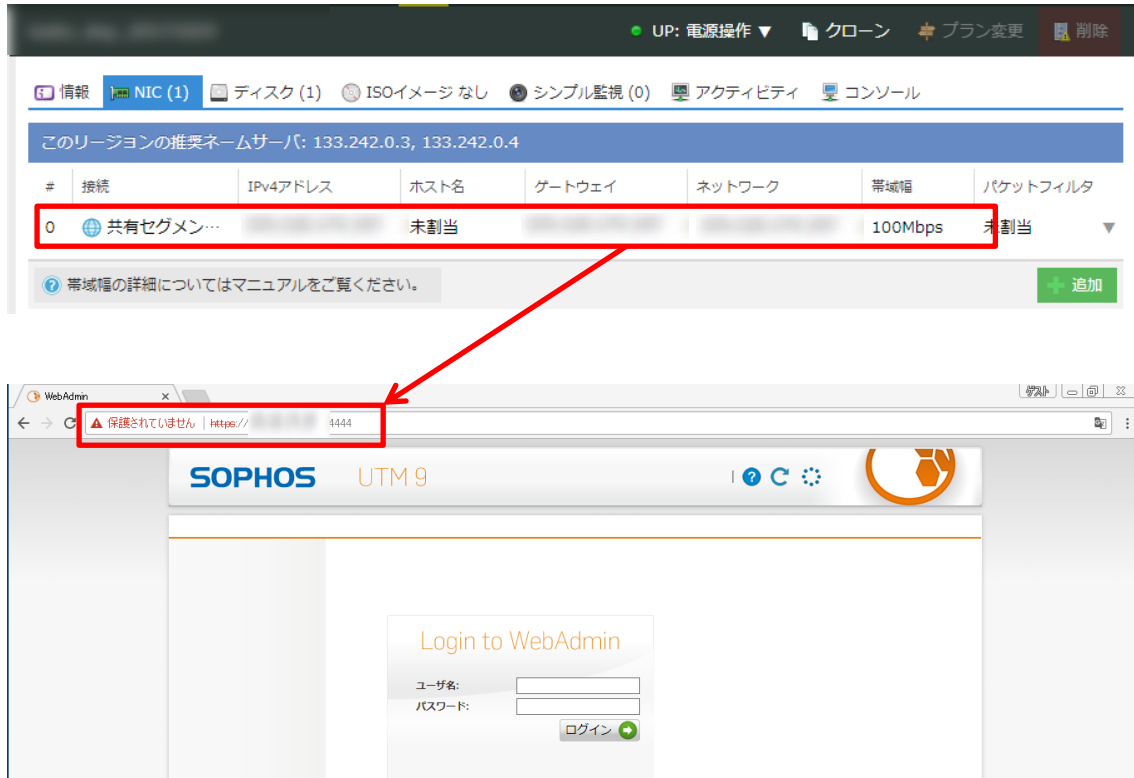
Sophos UTM
(C) Copyright 2000-2017 Sophos Limited and others. All rights reserved.
Sophos is a registered trademark of Sophos Limited and Sophos Group.
All other product and company names mentioned are trademarks or registered
trademarks of their respective owners.

For more copyright information look at /doc/astaro-license.txt
or http://www.astaro.com/doc/astaro-license.txt

NOTE: If not explicitly approved by Sophos support, any modifications
done by root will void your support.

sophos_utm_9:/root # cc reset_system_id
1
sophos_utm_9:/root #
```

⑮NIC（1）タブで割り当てられた IP アドレスを確認し、https://（IP アドレス）:4444
でアクセスします。



⑯admin アカウントでログインします。ログイン直後、利用規約が表示されます。必要事項を必ずご確認頂き、確認ボタンを押下することでダッシュボードにアクセスすることが可能です。
初期パスワードは「Ys15Vbt96L」です。



以上で、共有セグメントへの展開手順は完了です。

(2) IP アドレスの手動割り当て

ここでは任意の IP アドレスを割り振る手順を記載します。

※ (1) 共有セグメントへの展開手順①～⑭まで同様です。

※アーカイブを展開する際に、ルータ+スイッチへの接続が前提となります。

例：■割り当てたい IP アドレス：172.16.0.2/24

■デフォルトゲートウェイ：172.16.0.1/24

①CC モードに切り替えます。

```
#cc
```

```
sophos_utm_9:/root # cc
Confid command-line client. Maintainer: <Ingo.Schwarze@sophos.com>

Connected to 127.0.0.1:4472, SID = FcpANDXMKOBsxPQDoNJJ.
Available modes: MAIN OBJS RAW WIZARD.
Type mode name to switch mode.
Typing 'help' will always give some help.
-

```

②RAW モードに切り替えます。

```
#RAW
```

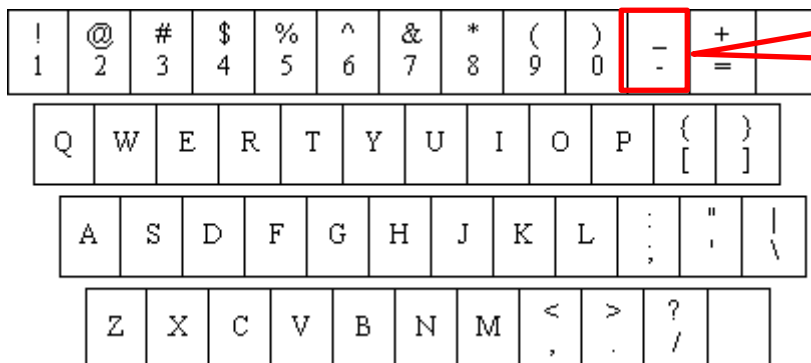
```
Connected to 127.0.0.1:4472, SID = PDRwCuAwYukVjlyZDDbB.
Available modes: MAIN OBJS RAW WIZARD.
Type mode name to switch mode.
Typing 'help' will always give some help.
RAW
Switched to RAW mode.

```

③書き換えを許可するコマンドを発行します。

ご注意：コンソールからの入力時、US キーボード配列仕様となっております。

「_」（アンダーバー）は Shift キーを押しながら以下の箇所で入力することができます。



日本語キーボードの「ほ」の位置に該当します。

※US キーボード配列

```
#lock_override
```



```
Connected to 127.0.0.1:4472, SID = WjbFrXaMapMoZfRXJzUY.
Available modes: MAIN OBJS RAW WIZARD.
Type mode name to switch mode.
Typing 'help' will always give some help.
      RAW
Switched to RAW mode.
      lock_override
Calling Confd function lock_override()
result: 1
```

④OBJS モードに切り替えます。

#OBJS

```
Switched to RAW mode.
      OBJS
Switched to OBJS mode.
```

⑤インターフェースの設定階層まで移動します。

ご注意：コンソールからの入力時、US キーボード配列仕様となっております。

[] (半角角カッコ) は以下の箇所で入力することができます。

!	@	#	\$	%	^	&	*	()	-	+	
1	2	3	4	5	6	7	8	9	0	-	=	
Q	W	E	R	T	Y	U	I	O	P	{	}	
										[]	
A	S	D	F	G	H	J	K	L	:	"	\	
									:	'	\	
Z	X	C	V	B	N	M	<	>	?			
							,	.	/			

日本語キーボードの「@」、
「[」の位置に該当します。

※US キーボード配列

```
127.0.0.1 OBJS > interface
127.0.0.1 OBJS interface > ethernet
127.0.0.1 OBJS interface ethernet > REF_DefaultInternal[External]
127.0.0.1 OBJS interface ethernet [REF_DefaultInternal] > REF_ItfParamsDefaultInternal
```

```
interface
  ethernet
    REF_DefaultInternal[External]
Logged into object 'REF_DefaultInternal'. Use 'w' to write eventual changes.
{
  'additional_addresses' => [],
  'bandwidth' => 100000000,
  'comment' => 'auto-created on installation',
  'inbandwidth' => 0,
  'itfhw' => 'REF_ItfHwDefaultInternal',
  'link' => 1,
  'mtu' => 1500,
  'mtu_auto_discovery' => 1,
  'name' => 'External',
  'outbandwidth' => 0,
  'primary_address' => 'REF_ItfParamsDefaultInternal',
  'proxyarp' => 0,
  'proxypdp' => 0,
  'status' => 1
}
```

```

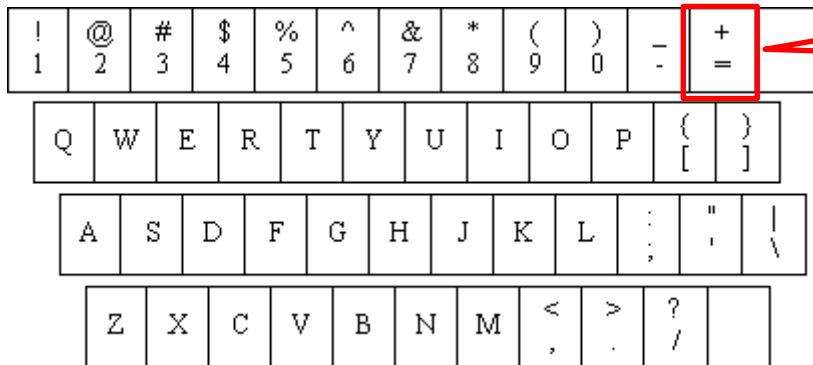
REF_ItfParamsDefaultInternal
Logged into object 'REF_ItfParamsDefaultInternal'. Use 'w' to write eventual changes.
{
  'address' => '172.16.0.2',
  'address6' => '::',
  'comment' => '',
  'default_gateway_address' => '172.16.0.1',
  'default_gateway_address6' => '::',
  'default_gateway_status' => 1,
  'default_gateway_status6' => 0,
  'dhcpv6_rapid_commit' => 0,
  'dns_server_1' => '0.0.0.0',
  'dns_server_2' => '0.0.0.0',
  'dns_server_3' => '::',
  'dns_server_4' => '::',
  'gateway_type' => 'dynamic',
  'gateway_type6' => 'static',
  'hostname' => '',
  'interface_address' => 'REF_DefaultInternalAddress',
  'interface_broadcast' => 'REF_DefaultInternalBroadcast',
  'interface_network' => 'REF_DefaultInternalNetwork',
  'name' => 'Internal',
  'netmask' => 24,
  'netmask6' => 64,
  'pd_address6' => '',
  'pd_netmask6' => 64,
  'pd_resolved6' => 0,
  'resolved' => 1,
  'resolved6' => 0,
  'six2four' => 0,
  'type' => 'dynamic',
  'type6' => 'static'
}

```

⑥IP アドレスを書き換えます。

ご注意：コンソールからの入力時、US キーボード配列仕様となっております。

= (イコール) は以下の箇所で入力することができます。



日本語キーボードの「へ」
の位置に該当します。

※US キーボード配列

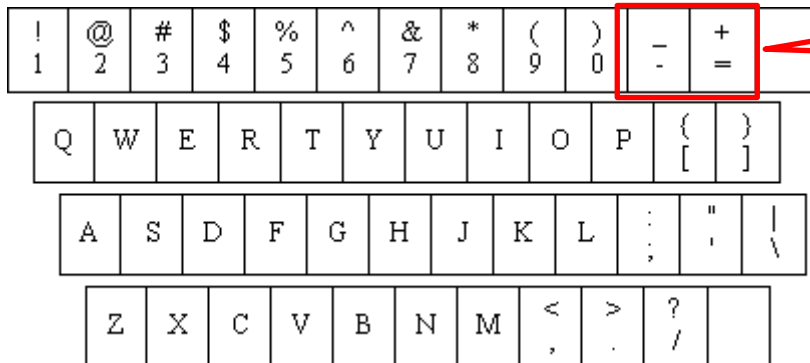
127.0.0.1 OBJS interface ethernet [REF_ItfParamsDefaultInternal] > **address=172.16.0.2**

```
{
  'address' => ' 172.16.0.2 ',
  'address6' => ':::',
  'comment' => '',
  'default_gateway_address' => ' ',
  'default_gateway_address6' => '',
  'default_gateway_status' => 1,
  'default_gateway_status6' => 0,
  'dhcpv6_rapid_commit' => 0,
  'dns_server_1' => '0.0.0.0',
  'dns_server_2' => '0.0.0.0',
  'dns_server_3' => ':::',
  'dns_server_4' => ':::',
  'gateway_type' => 'dynamic',
  'gateway_type6' => 'static',
  'hostname' => '',
  'interface_address' => 'REF_DefaultInternalAddress',
  'interface_broadcast' => 'REF_DefaultInternalBroadcast',
  'interface_network' => 'REF_DefaultInternalNetwork',
  'name' => 'Internal',
  'netmask' => 24,
  'netmask6' => 64,
  'pd_address6' => '',
  'pd_netmask6' => 64,
  'pd_resolved6' => 0,
}
```

⑦デフォルトゲートウェイを書き換えます。

ご注意：コンソールからの入力時、US キーボード配列仕様となっております。

「_」(アンダーバー)、「=」(イコール) は以下の箇所を入力することができます。



日本語キーボードの「ほ」「へ」の位置に該当します。

※US キーボード配列

```
127.0.0.1 OBJS interface ethernet [REF_ItfParamsDefaultInternal] > default_gateway_address=172.16.0.1
```

```

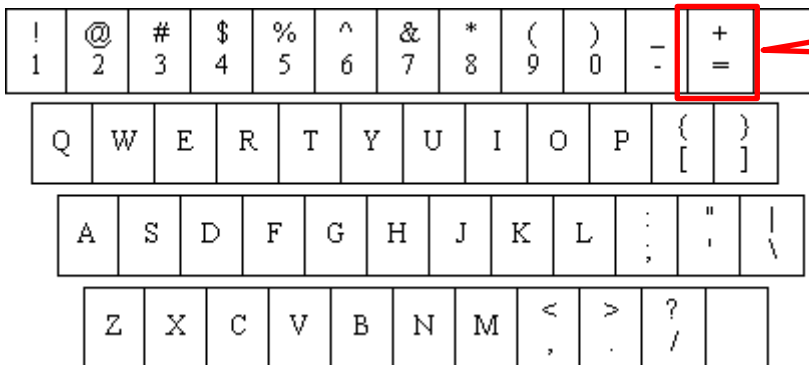
'address' => 172.16.0.2
'address6' =>
'comment' =>
'default_gateway_address' => '172.16.0.1'
'default_gateway_address6' =>
'default_gateway_status' => 1,
'default_gateway_status6' => 0,
'dhcpv6_rapid_commit' => 0,
'dns_server_1' => '0.0.0.0',
'dns_server_2' => '0.0.0.0',
'dns_server_3' => '::',
'dns_server_4' => '::',
'gateway_type' => 'dynamic',
'gateway_type6' => 'static',
'hostname' => '',
'interface_address' => 'REF_DefaultInternalAddress',
'interface_broadcast' => 'REF_DefaultInternalBroadcast',
'interface_network' => 'REF_DefaultInternalNetwork',
'name' => 'Internal',
'netmask' => 24,
'netmask6' => 64,
'pd_address6' => '',
'pd_netmask6' => 64,
'pd_resolved6' => 0,
'resolved' => 1,
'resolved6' => 0,
'sixfour' => 0,
'type' => 'dynamic',
'type6' => 'static'

```

⑧IP アドレスのタイプを Static に書き換えます。

ご注意：コンソールからの入力時、US キーボード配列仕様となっております。

「=」（イコール）は以下の箇所を入力することができます。



日本語キーボードの「へ」
の位置に該当します。

※US キーボード配列

```
127.0.0.1 OBJS interface ethernet [REF_ItfParamsDefaultInternal] > type=static
```

```

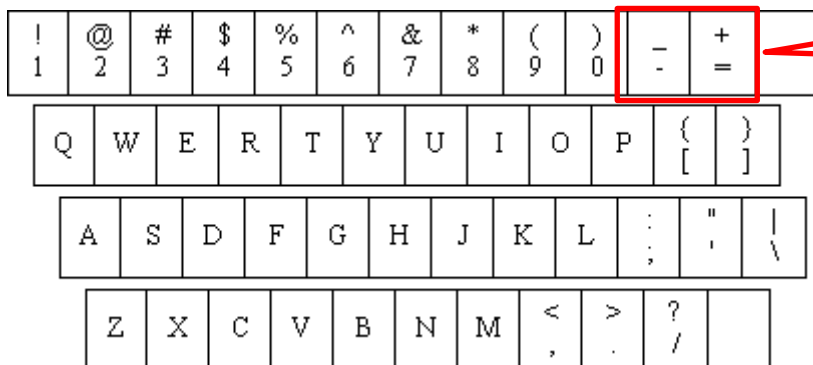
type=static
{
  'address' => '...',
  'address6' => ':::',
  'comment' => '',
  'default_gateway_address' => '...',
  'default_gateway_address6' => ':::',
  'default_gateway_status' => 1,
  'default_gateway_status6' => 0,
  'dhcpv6_rapid_commit' => 0,
  'dns_server_1' => '0.0.0.0',
  'dns_server_2' => '0.0.0.0',
  'dns_server_3' => ':::',
  'dns_server_4' => ':::',
  'gateway_type' => 'dynamic',
  'gateway_type6' => 'static',
  'hostname' => '',
  'interface_address' => 'REF_DefaultInternalAddress',
  'interface_broadcast' => 'REF_DefaultInternalBroadcast',
  'interface_network' => 'REF_DefaultInternalNetwork',
  'name' => 'Internal',
  'netmask' => 24,
  'netmask6' => 64,
  'pd_address6' => '',
  'pd_netmask6' => 64,
  'pd_resolved6' => 0,
  'resolved' => 1,
  'resolved6' => 0,
  'sixfour' => 0,
  'type' => 'static',
  'type6' => 'static'
}

```

⑨ゲートウェイアドレスのタイプを Static に書き換えます。

ご注意：コンソールからの入力時、US キーボード配列仕様となっております。

「_」(アンダーバー)、「=」(イコール) は以下の箇所で入力することができます。



※US キーボード配列

127.0.0.1 OBJS interface ethernet [REF_ItfParamsDefaultInternal] > **gateway_type=static**

```
gateway_type=static
{
  'address' =>
  'address6' =>
  'comment' => '',
  'default_gateway_address' =>
  'default_gateway_address6' =>
  'default_gateway_status' => 1,
  'default_gateway_status6' => 0,
  'dhcpv6_rapid_commit' => 0,
  'dns_server_1' => '0.0.0.0',
  'dns_server_2' => '0.0.0.0',
  'dns_server_3' => ':::',
  'dns_server_4' => ':::',
  'gateway_type' => 'static',
  'gateway_type6' => 'static',
  'hostname' => '',
  'interface_address' => 'REF_DefaultInternalAddress',
  'interface_broadcast' => 'REF_DefaultInternalBroadcast',
  'interface_network' => 'REF_DefaultInternalNetwork',
  'name' => 'Internal',
  'netmask' => 24,
  'netmask6' => 64,
  'pd_address6' => '',
  'pd_netmask6' => 64,
  'pd_resolved6' => 0,
  'resolved' => 1,
  'resolved6' => 0,
  'sixfour' => 0,
  'type' => 'static',
  'type6' => 'static'
}
```

⑩変更を保存し、save が成功することを下記のメッセージにて確認します。

```
127.0.0.1 OBJS interface ethernet [REF_ItfParamsDefaultInternal] > w
```

Change to object saved successfully

```
Changes to object saved successfully.
{
  'address' =>
  'address6' => ':::',
  'comment' => '',
  'default_gateway_address' =>
  'default_gateway_address6' => '',
  'default_gateway_status' => 1,
  'default_gateway_status6' => 0,
  'dhcpv6_rapid_commit' => 0,
  'dns_server_1' => '0.0.0.0',
  'dns_server_2' => '0.0.0.0',
  'dns_server_3' => ':::',
  'dns_server_4' => ':::',
  'gateway_type' => 'static',
  'gateway_type6' => 'static',
  'hostname' => '',
  'interface_address' => 'REF_DefaultInternalAddress',
  'interface_broadcast' => 'REF_DefaultInternalBroadcast',
  'interface_network' => 'REF_DefaultInternalNetwork',
  'name' => 'Internal',
  'netmask' => 24,
  'netmask6' => 64,
  'pd_address6' => '',
  'pd_netmask6' => 64,
  'pd_resolved6' => 0,
  'resolved' => 1,
  'resolved6' => 0,
  'sixfour' => 0,
  'type' => 'static',
  'type6' => 'static'
}
```

⑪CC コマンドを終了します。

```
127.0.0.1 OBJS interface ethernet [REF_ItfParamsDefaultInternal] > exit
```

⑫再起動します。

#reboot

⑬手動で割り当てた IP アドレスで、https:// (IP アドレス) :4444 へアクセスします。

⑭利用規約同意後、ダッシュボードへアクセス可能となります。

以上で、IP アドレスの手動割り当て手順は完了です。

(3) ライセンスサーバに接続する手順

※利用規約同意後、ダッシュボードへのアクセスができた時点より手順を記載します。

①左メニューのマネジメント > 集中管理 (SUM) を押下し、画面右上のスイッチを押下します。



②SUM ホストのフォルダアイコンを押下します。左メニューよりライセンスサーバ情報をドラック&ドロップします。ライセンスサーバは「license.owlook.ne.jp」です。



③適用を押下すると、設定が保存されます。保存されたタイミングで右上のボタンが緑に変わります。

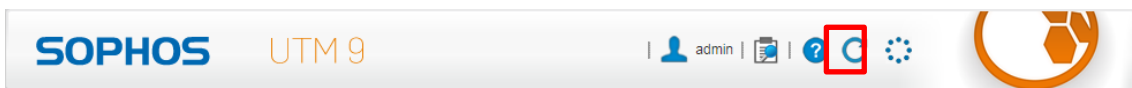


④画面中段の SUM のステータスに以下のメッセージが出ていれば接続成功です。

メッセージ : Login for [1] successful.



画面の情報を更新する際は以下のボタンを押下します。



⑤しばらくするとフルガードライセンスに切り替わります。

切替前のライセンス状況（ダッシュボード右下より）

グレイアウトしている機能はライセンス自体が無効です。有効にすることはできません。



切替後のライセンス状況

赤で表記されているのは、機能としては無効ですが、ライセンスとしては有効です。



以上で、ライセンスサーバに接続する手順は完了です。

(4) サービス終了手順

ライセンスサーバに接続し、ライセンスが有効状態になると、管理画面からライセンスの操作が一切できなくなります。本手順は本サービスの利用を終了させる場合に実施してください。

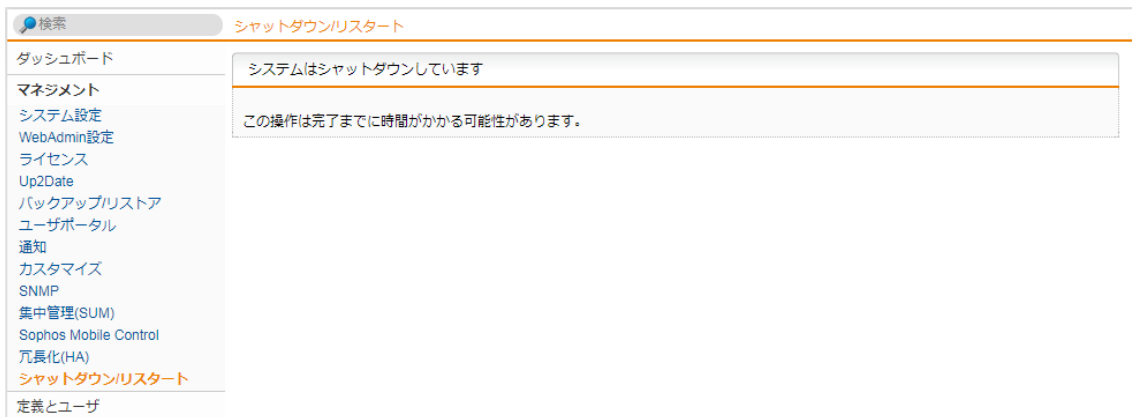


本サービスを終了するためには、Sophos UTM9 のインスタンスを削除する必要があります。削除手順は、さくらのクラウド上の管理画面から行います。

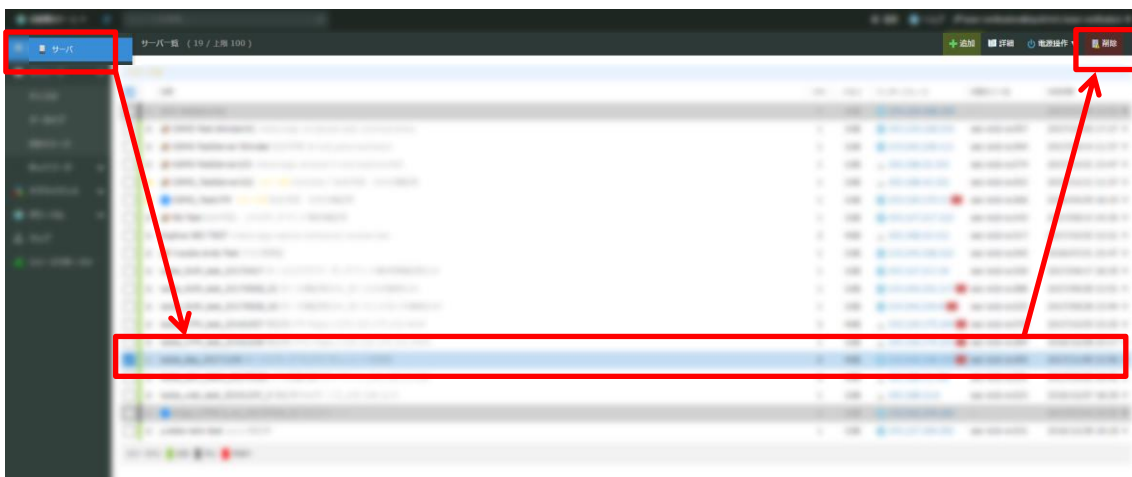
①SophosUTM9 の管理画面左メニューのマネジメント > シャットダウン/リスタート よりシステムをシャットダウン（停止）を押下します。



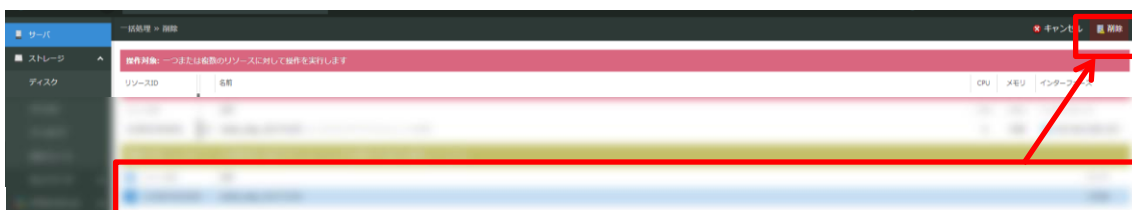
画面が遷移し「システムはシャットダウンしています」画面に遷移します。



②さくらのクラウド管理画面の左メニュー「サーバ」から該当のインスタンスを選択し、「削除」ボタンを押下します。



③削除画面に遷移するので、該当の Disk をチェックし、Disk も含めて削除します。



④該当のインスタンスが削除された時点で、ライセンスは無効となり、本サービスのご利用も終了となります。

以上で、サービス終了手順は完了です。

4. 初期設定

4-1. Sophos UTM9 の初期設定

(1) UTM の基本情報変更手順

ここでは組織情報、管理者メールアドレス、UTM ホスト名の変更を行います。

① マネジメント > システム設定 > 組織タブを押下します。

組織名、市区町村、管理者メールアドレスの情報を入力します。

ダッシュボード

組織 **ホスト名** 日付と時刻 シェアアク... スキャン設定 設定またはパス...

マネジメント

システム設定

WebAdmin設定

ライセンス

Up2Date

バックアップ/リストア

ユーザポータル

通知

カスタマイズ

SNMP

集中管理(SUM)

Sophos Mobile Control

冗長化(HA)

シャットダウン/リスタート

組織情報

組織名: null

市区町村: null

国: Japan

管理者メールアドレス

あなたの組織の名前と場所を設定してください。IPsec、メール暗号化、WebAdmin用の証明書にもこのデータは使用されます。

適用

② 続いてホスト名タブを押下します。

任意のホスト名の情報を入力します。

ダッシュボード

組織 **ホスト名** 日付と時刻 シェアアク... スキャン設定 設定またはパス...

マネジメント

システム設定

WebAdmin設定

ライセンス

Up2Date

バックアップ/リストア

ユーザポータル

通知

カスタマイズ

SNMP

集中管理(SUM)

Sophos Mobile Control

冗長化(HA)

シャットダウン/リスタート

システムDNSホスト名

ホスト名: sophos_utm_9.5

これはシステムのホスト名です。ドメインを含んだFQDN形式で設定し、公開されているDNSでシステムの外部インタフェースとして解決されるようにしてください。DynDNSをご利用の場合はDynDNSホスト名を使用してください。

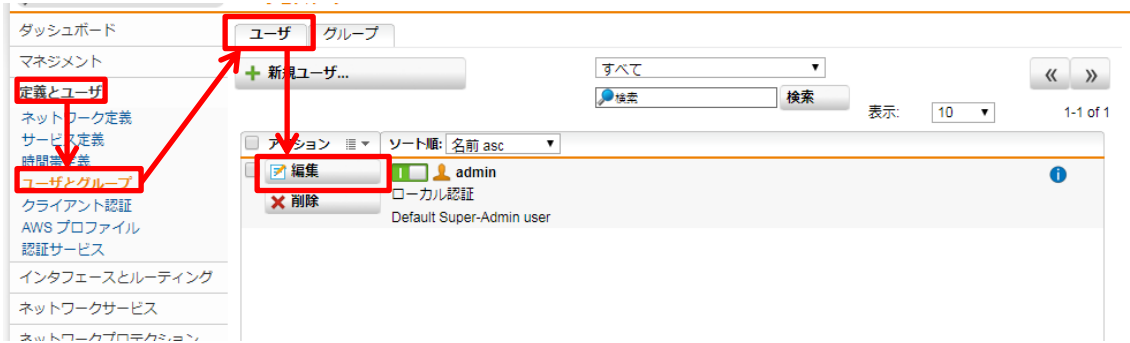
適用

以上で、UTM の基本情報変更手順は完了です。

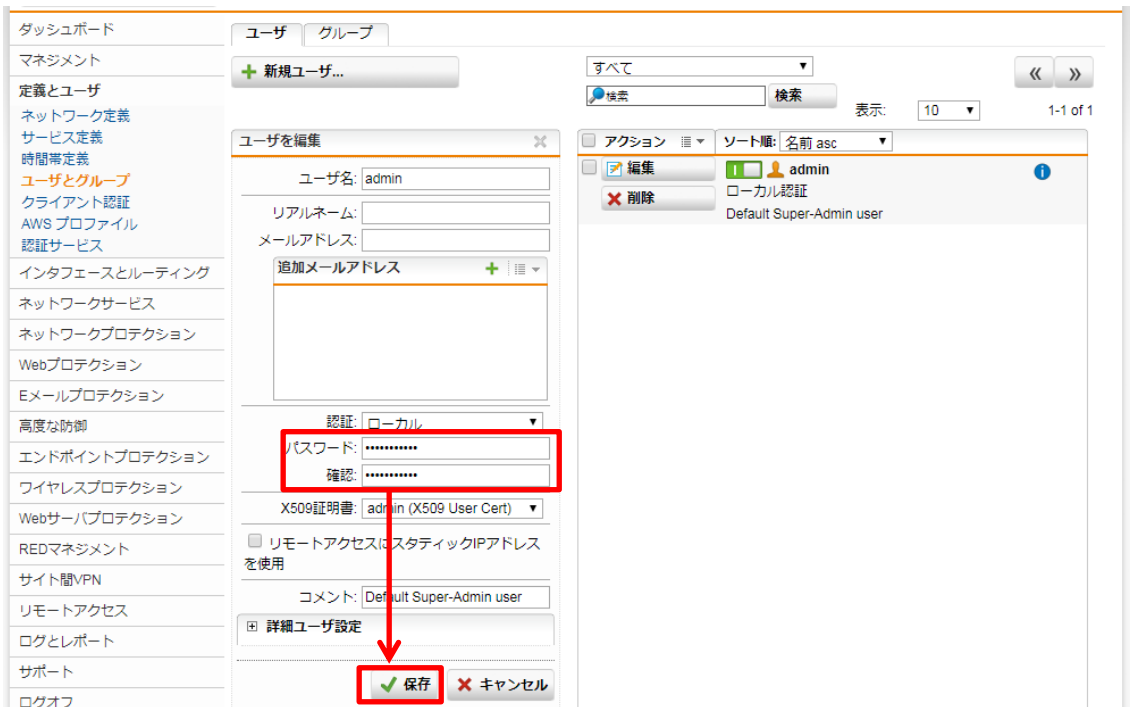
(2) 管理者パスワード変更手順

①定義とユーザ > ユーザとグループ > ユーザタブを押下します。

admin ユーザの編集ボタンを押下します。



②編集画面より、パスワード、確認項目に新たなパスワードを入力し、保存ボタンを押下します。

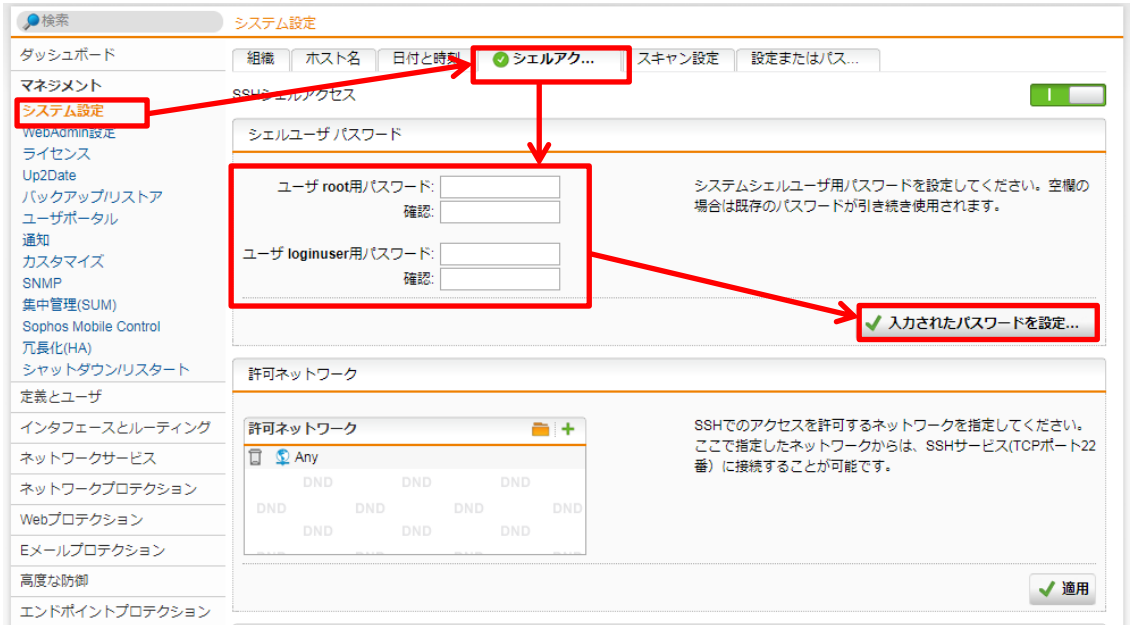


以上で、管理者パスワード変更手順は完了です。

(3) Shell アクセス (SSH) のパスワード変更変更手順

① マネジメント > システム設定 > シェルアクセスタブを押下します。

ユーザ root 用パスワード、確認及びユーザ loginuser 用パスワード、確認項目に新たなパスワードを入力し、入力されたパスワードを設定するを押下します。



② シェルアクセス自体を無効にする場合は右上のボタンを押下します。

グレイアウトされるとシェルアクセスが無効化されます。



シェルアクセスは必要でない限り無効にすることを推奨します。

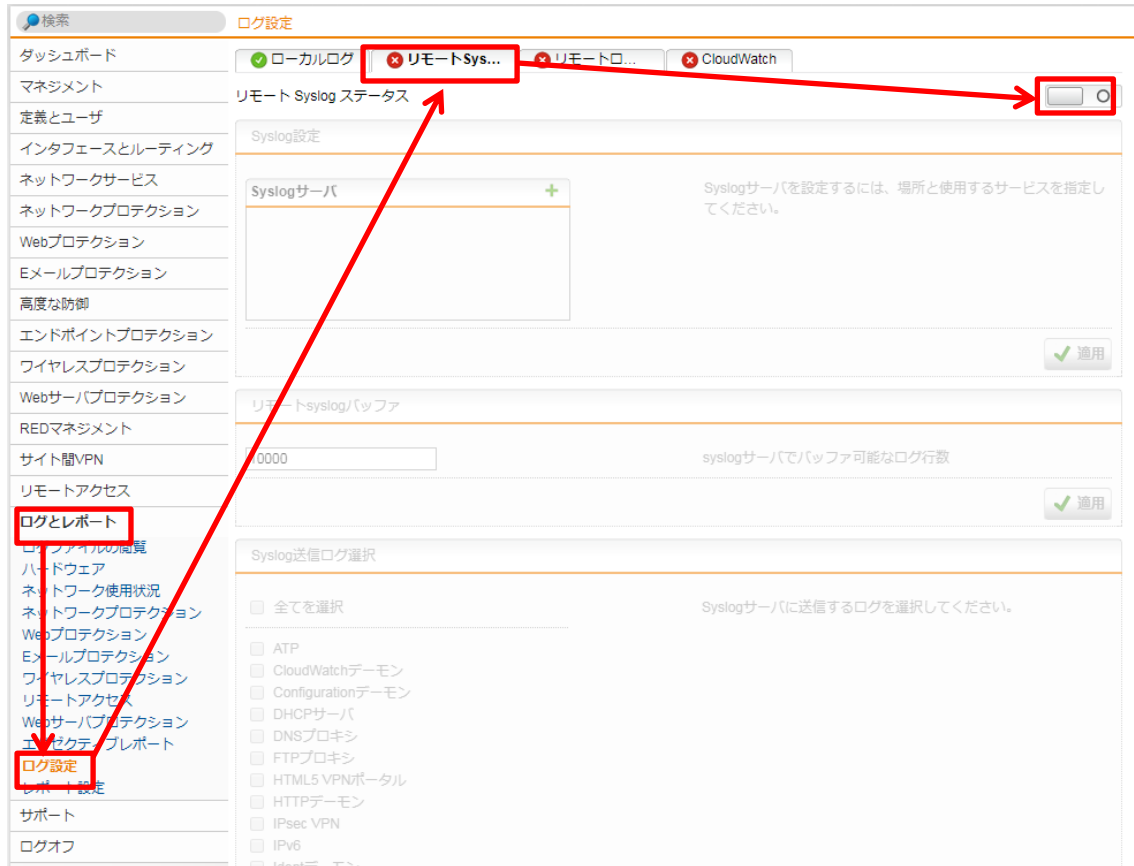
以上で、Shell アクセス (SSH) のパスワード変更変更手順は完了です。

(4) Syslog 連携手順

Syslog サーバは利用者にて用意する必要があります。本手順は必要な場合のみ実施してください。

①ログとレポート > ログ設定 > リモート Syslog タブを押下します。

右上の有効化ボタンを押下します。



②Syslog 設定項目で「+」ボタンを押下し Syslog サーバの情報を入力します。



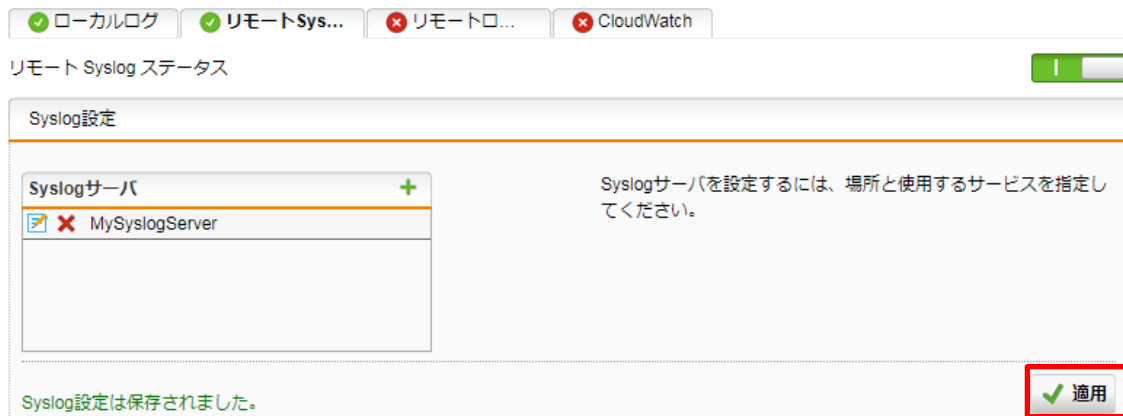
③以下のようなポップアップ画面が出力されます。

サーバ、ポート項目のそれぞれの「+」ボタンを押下すと、さらにポップアップ画面が出力されます。必要な値を入力し保存ボタンを押下します。



④Syslog 設定項目に③で設定したサーバ情報が登録されます。

適用ボタンを押下します。



⑤Syslog 送信ログ選択項目で、Syslog サーバに転送したいカテゴリを選択し、適用ボタンを押下します。



以上で、Syslog 連携手順は完了です。

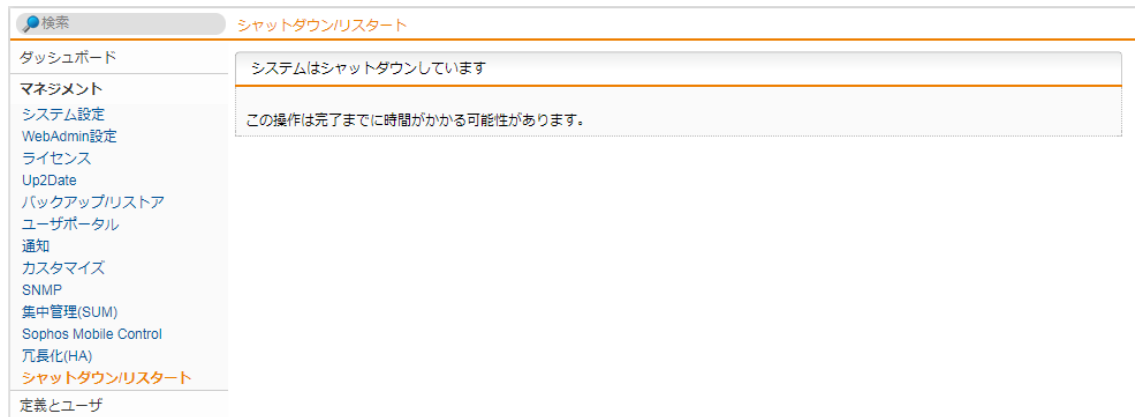
(5) NICを追加しIPアドレスを割り当て手順

Sophos UTM9はアクティベートされた初期状態でInternalインターフェースが作成されています。ご利用いただくために、Internalインターフェースを有効にし、スイッチへの接続設定を行います。

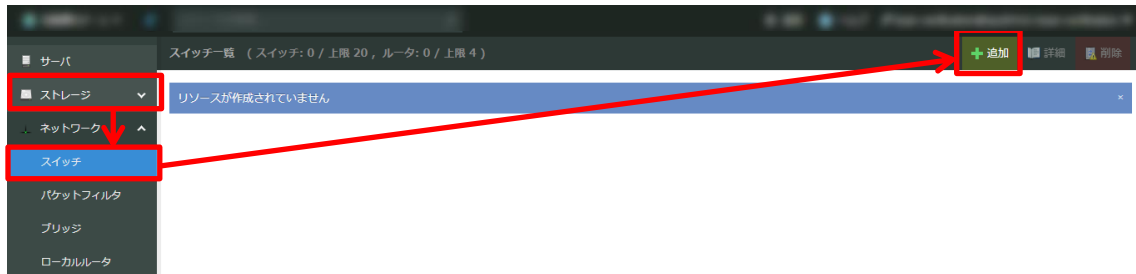
①SophosUTM9の管理画面左メニューのマネジメント > シャットダウン/リスタート よりシステムをシャットダウン（停止）を押下します。



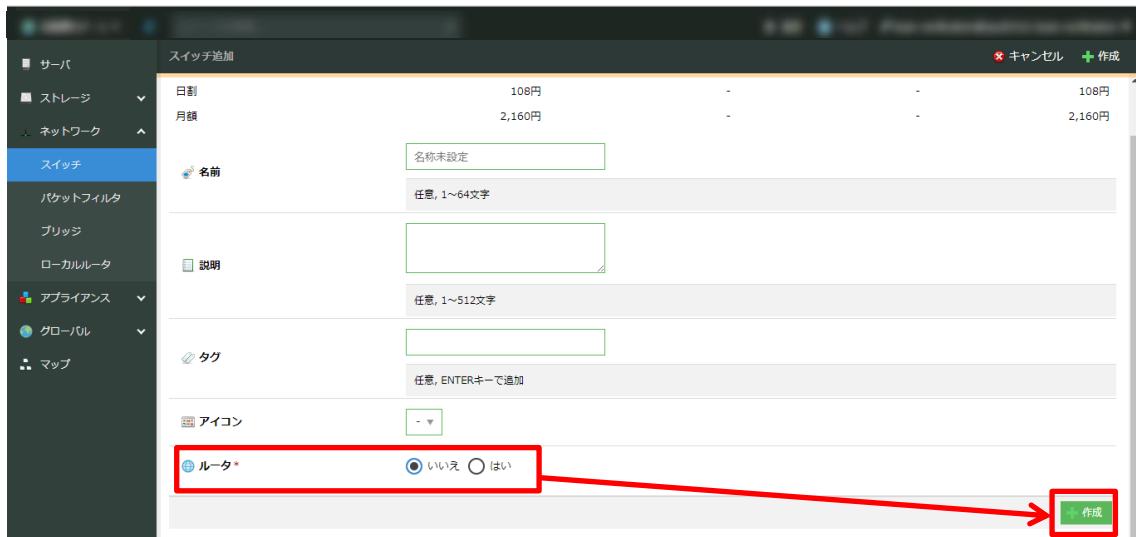
画面が遷移し「システムはシャットダウンしています」画面に遷移します。



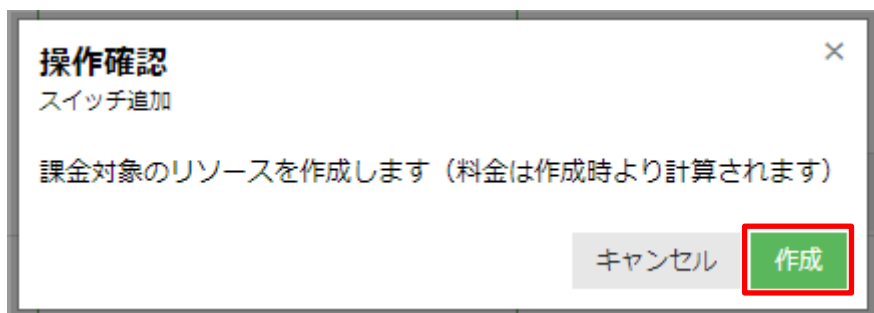
②さくらのクラウドコントロールパネルよりスイッチ追加の手続きを行います。ネットワークメニューよりスイッチを選択し、追加ボタンを押下し、スイッチの追加手続きを行います。ここで作成されるスイッチはさくらのクラウドが提供する有料のサービスです。



必要な項目を入力します。この時、ルータの項目は「いいえ」を選択し、作成ボタンを押下します。



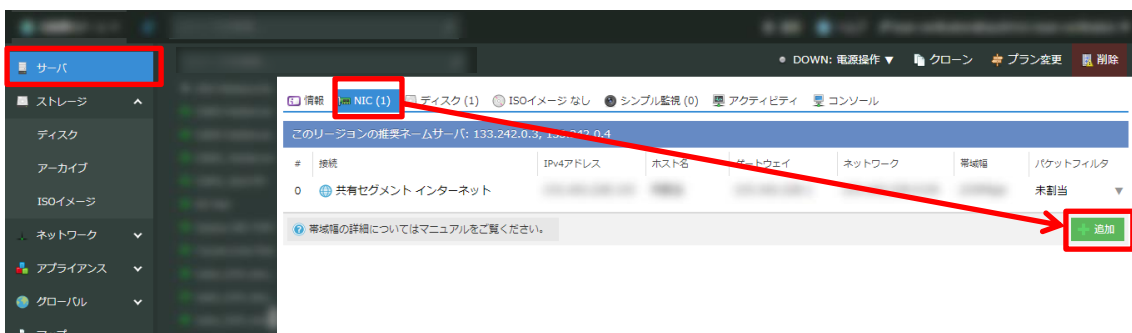
確認メッセージで追加を押下し、スイッチ追加プロセスを実行します。



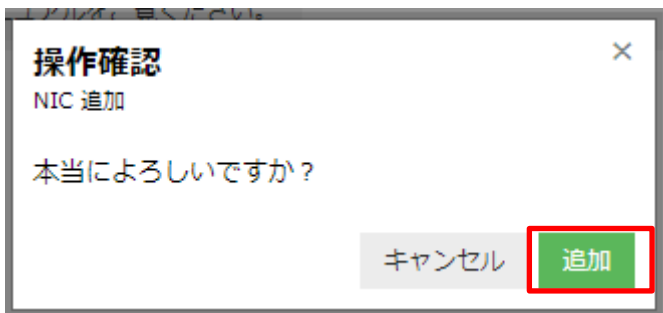
名前	メソッド	リソース	ステータス
スイッチ: 作成	POST	cloud/1.1/switch	成功

中断 閉じる

③Sophos UTM9 が停止したら、さくらのクラウドコントロールパネルより NIC 追加の手続きを行います。サーバメニューより、Sophos UTM9 のインスタンスを選択し、詳細 > NIC > 追加 を押下します。



確認メッセージで追加を押下し、NIC 追加プロセスを実行します。



NIC 追加プロセスが成功したことを確認します。

名前	メソッド	リソース	ステータス
NIC追加	POST	cloud/1.1/interface	成功

中断 閉じる

④追加した新規 NIC を②手順で作成したスイッチに接続します。

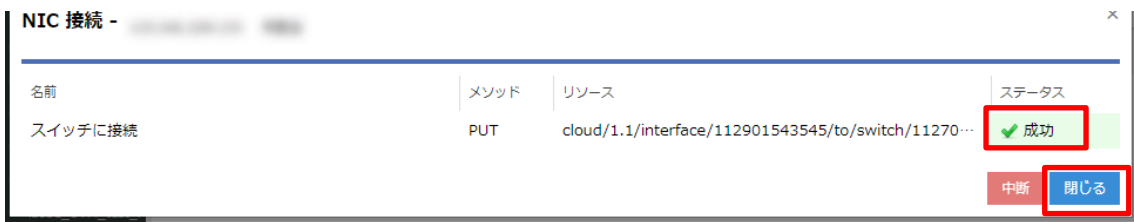
「1 未接続」の NIC 列の最右のメニューを展開し、接続を編集を押下します。



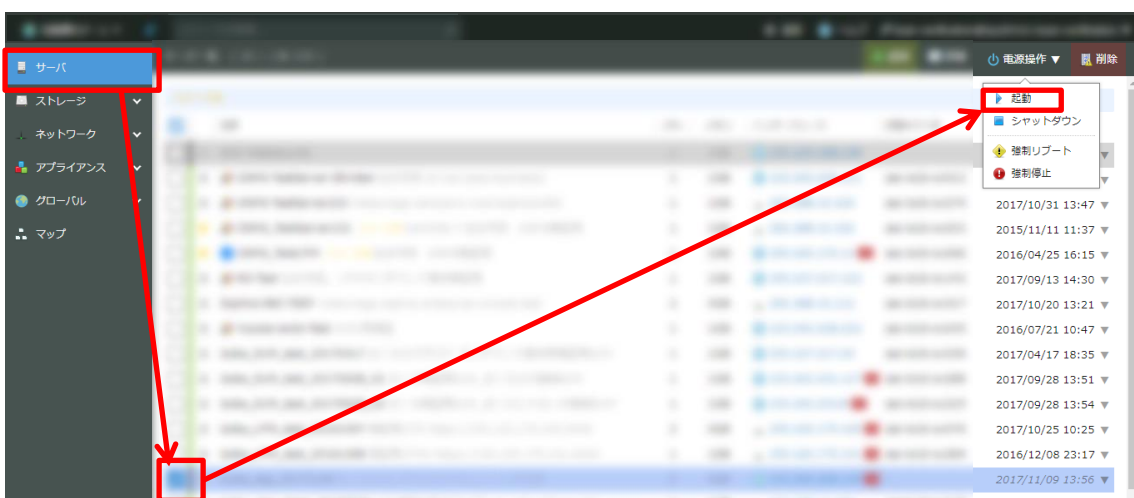
スイッチに接続を選択し、②手順で作成したスイッチを選択し更新を押下します。



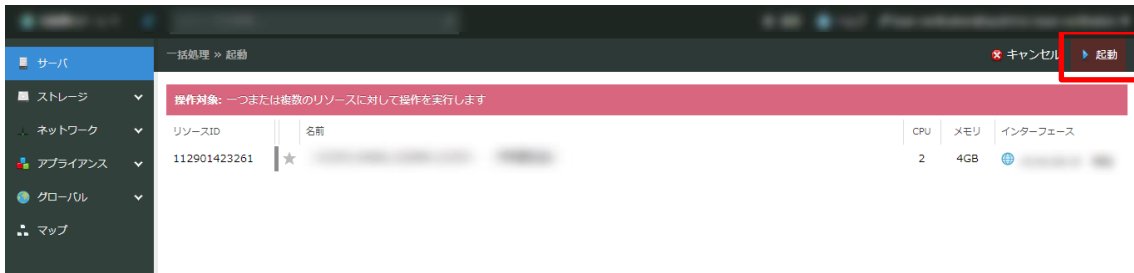
NIC 接続プロセスが成功したことを確認します。



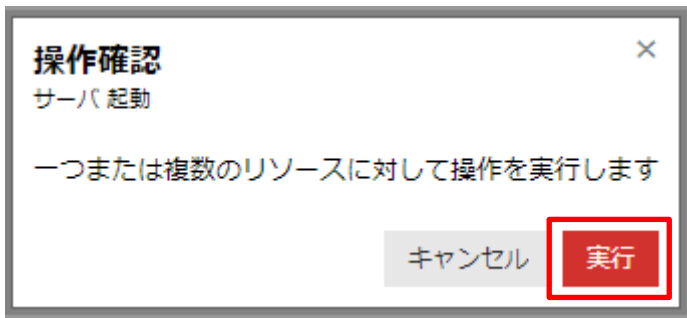
⑤さくらのクラウドコントロールパネルより Sophos UTM9 のインスタンスの起動処理を行います。サーバメニューより、Sophos UTM9 のインスタンスを選択し、電源操作 > 起動 を押下します。



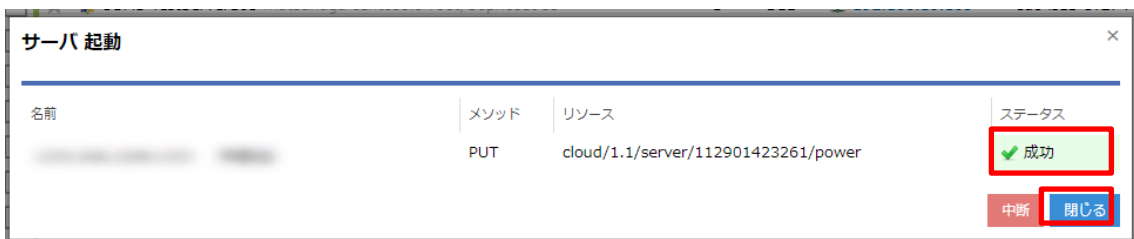
確認画面から、起動ボタンを押下します。



確認画面より実行ボタンを押下します。

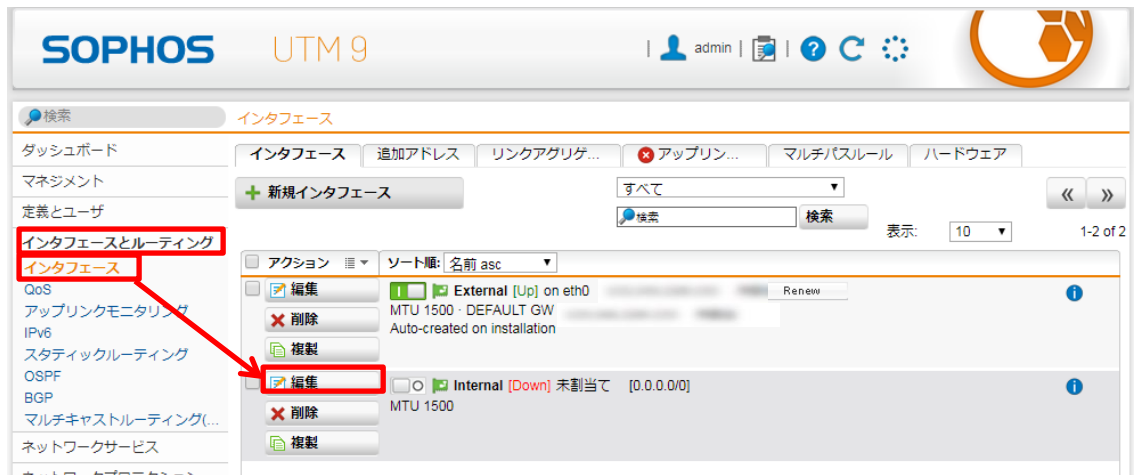


サーバ起動プロセスが成功したことを確認します。



⑥Sophos UTM9 の起動が完了したら、インターフェースの設定を行います。

管理画面へアクセスし、インターフェースとルーティング > インターフェイス 画面へ遷移し
Internal インターフェイスの編集を押下します。



編集画面から以下の通り、設定を入力し、保存ボタンを押下します。

タイプ：イーサネット

ハードウェア：eth1 Virtio network device ※新たに追加した NIC

動的 IPv4：チェックなし

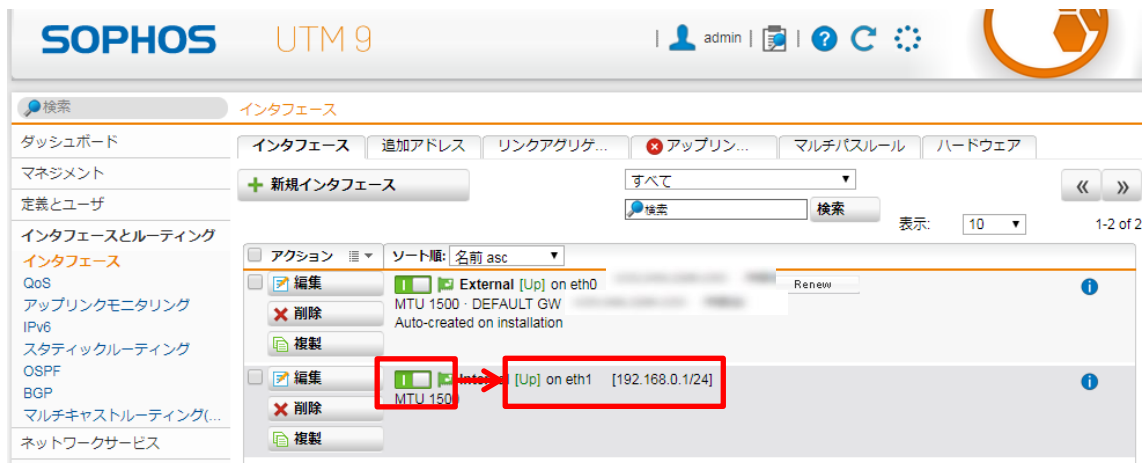
IPv4 アドレス：192.168.0.1

IPv4 ネットマスク：/24 (255.255.255.0)

IPv4 デフォルト GW：チェックなし



ステータスボタンを押下し、「UP」状態になることを確認します。



以上で、NIC を追加し IP アドレスを割り当て手順は完了です。

(6) マニュアル参照手順

④UTM の OS 内部にオンラインヘルプ機能が具備されており、必要なときに閲覧が可能です。
画面の上部フレーム内の「？」マークを押下します。

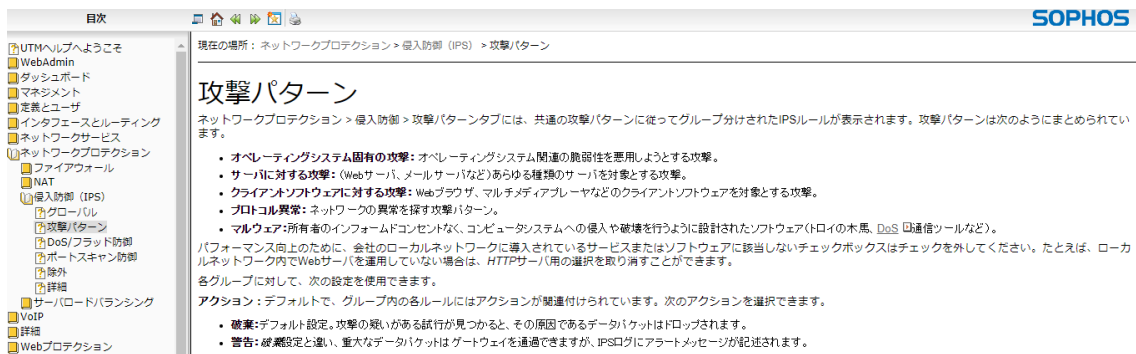
以下のようなオンラインヘルプが別タブで開きます。

オンラインヘルプが必要な個所をすぐに開くことができます。

例えば、ネットワークプロテクションのIPS機能の攻撃パターンの設定で確認したい事があるとします。以下の画面から「？」マークを押下すると



直接攻撃パターンについてのオンラインヘルプにアクセスすることが可能です。



以上で、マニュアル参照手順は完了です。

(7) バックアップ取得手順

① マネジメント > バックアップ/リストア > バックアップ/リストアタブより
バックアップを直ちに作成を押下します。

The screenshot shows the Sophos UTM management interface. On the left, the 'Management' menu is expanded to 'Backup/Restore'. The main area displays a table of 'Usable Backups' and a 'Create Backup' section. A red box highlights the 'Backup/Restore' menu item, and another red box highlights the 'Create Backup' button. A red arrow points from the 'Backup/Restore' menu to the 'Create Backup' button.

利用可能なバックアップ	作成日時	バージョン	作成者
<input type="checkbox"/>	2017-10-26 10:59	9.503-4	admin
<input type="checkbox"/>	2017-10-19 09:52	9.500-9	system
<input type="checkbox"/>	Automatic Backup (Up2Date 9.503004)	9.500-9	system
<input type="checkbox"/>	Automatic Backup (Up2Date 9.502004)	9.500-9	system
<input type="checkbox"/>	2017-10-19 09:48	9.500-9	system
<input type="checkbox"/>	Automatic Backup (Up2Date 9.501005)		

バックアップの作成

コメント (任意):

バックアップを作成する際に削除するデータ:

- サイト固有情報 (ライセンス、パスワード、証明書/鍵、エンドポイント情報)
- 管理者メールアドレス。

バックアップ作成を実行すると現在の設定が保存され、利用可能なバックアップのリストに追加されます。作成の際、オプションでコメントを付けることができます。

② 取得したバックアップが利用可能なバックアップの一覧に追加されます。

The screenshot shows the same Sophos UTM management interface as above, but now the 'Usable Backups' table includes two new entries. A red box highlights these two new entries.

利用可能なバックアップ	作成日時	バージョン	作成者
<input type="checkbox"/>	2017-10-26 10:46	9.503-4	admin
<input type="checkbox"/>	(resetting host data to the defaults)		
<input type="checkbox"/>	2017-10-26 09:47	9.503-4	admin
<input type="checkbox"/>	(resetting host and mail data to the defaults)		
<input type="checkbox"/>	2017-10-19 09:52	9.500-9	system
<input type="checkbox"/>	Automatic Backup (Up2Date 9.503004)		
<input type="checkbox"/>	2017-10-19 09:50	9.500-9	system
<input type="checkbox"/>	Automatic Backup (Up2Date 9.502004)		
<input type="checkbox"/>	2017-10-19 09:48	9.500-9	system
<input type="checkbox"/>	Automatic Backup (Up2Date 9.501005)		

③ リストの横にあるアイコンで、以下のボタンを押下することで、バックアップファイルをダウンロードすることが可能です。



またメールアイコンで任意の宛先にファイルを送信することが可能です。



以上で、バックアップ取得手順は完了です。

(8) リストア手順

① マネジメント > バックアップ/リストア > バックアップ/リストアタブより
バックアップのインポートを押下します。

バックアップ/リストア

利用可能なバックアップ	作成日時	バージョン	作成者
<input type="checkbox"/>	2017-10-19 09:52	9,500-9	system
	Automatic Backup (Up2Date 9.503004)		
<input type="checkbox"/>	2017-10-19 09:50	9,500-9	system
	Automatic Backup (Up2Date 9.502004)		
<input type="checkbox"/>	2017-10-19 09:48	9,500-9	system
	Automatic Backup (Up2Date 9.501005)		

バックアップの作成

コメント (任意):

バックアップを作成する際に削除するデータ:

- サイト固有情報 (ライセンス、パスワード、証明書、鍵、エンドポイント情報)
- 管理者メールアドレス。

バックアップのインポート

バックアップファイル:

パスワード:

② フォルダアイコンを押下しバックアップファイルをアップロードします。

バックアップのインポート

バックアップファイル:

パスワード:

ファイルを選択

アップロード開始

バックアップのインポート

バックアップファイル: 

パスワード:

















既存のバックアップをアップロードします。リストアは行われず、バックアップリストに追加されます。

バックアップのインポート

③バックアップファイルがアップロードされると利用可能なバックアップの一覧に追加されます。

ダッシュボード

バックアップリ... 自動バック...

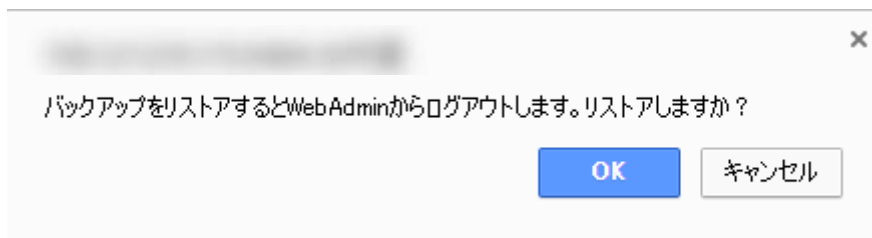
利用可能なバックアップ	作成日時	バージョン	作成者
<input type="checkbox"/>    	2017-10-26 10:46 <small>(resetting host data to the defaults)</small>	9.503-4	admin
<input type="checkbox"/>    	2017-10-19 09:52 <small>Automatic Backup (Up2Date 9.503004)</small>	9.500-9	system
<input type="checkbox"/>    	2017-10-19 09:50 <small>Automatic Backup (Up2Date 9.502004)</small>	9.500-9	system
<input type="checkbox"/>    	2017-10-19 09:48 <small>Automatic Backup (Up2Date 9.501005)</small>	9.500-9	system

選択したスナップショットの削除

④リストアボタンを押下します。



リストアボタンを押下すると、WebAdmin から自動的にログアウトします。

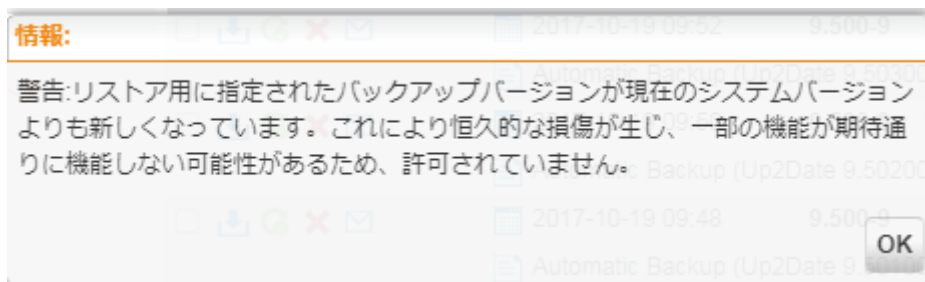


UTM の IP アドレスに変更がない場合（静的に割り当てている等）は即時反映されます。IP アドレスが変更となる場合は、リストア後に 60 秒ほど待ち、コンソールから UTM を再起動します。

#reboot

```
sophos_utm_9:/root # reboot
Broadcast message from root (tty1) (Thu Oct 26 10:53:48 2017):
The system is going down for reboot NOW!
INIT: Switching to runlevel: 6
INIT: Sending processes the TERM signal
INIT: Sending processes the KILL signal
blugd: can not set console device to /dev/pts/0: Device or resource busy
Master Resource Control: previous runlevel: 3, switching to runlevel:
:: Stopping WebAdmin 6
:: Shutting down acpid done
:: Stopping Configuration daemon done
:: Stopping Confd queue runner done
:: Stopping Confd request queuing daemon done
:: Stopping Cron done
:: Shutting down D-Bus daemon done
```

⑤再度、WebAdmin にログインしバックアップ内容が反映されていることを確認します。
またリストアに際して、UTM のバージョンが同一でないとリストアすることができません。



以上で、リストア手順は完了です。

冗長またはバックアップについての注意事項

さくらのクラウド環境では、Sophos UTM9 に搭載された HA クラスタ環境を構成することはできません。また、Sophos UTM9 のインスタンスに対する、アーカイブの取得によるバックアップですが、ご利用状況によってはライセンス違反となる可能性があります。

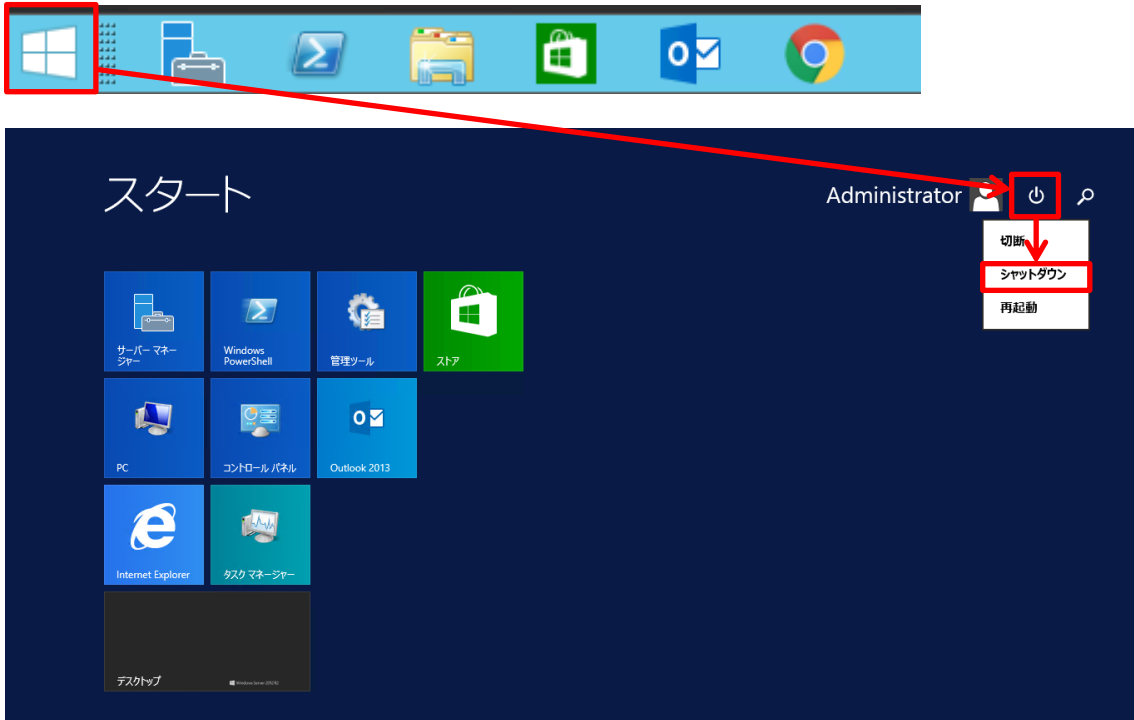
バックアップについては、Sophos UTM9 が提供するコンフィグバックアップをご利用いただき、復元についてはパブリックアーカイブより初期展開を行って頂く事を推奨します。

4-2. 保護対象システム（WindowsServer2012R2）の初期設定

保護対象システムを Sophos UTM9 で保護するためには、インターネットへのアクセスを必ず Sophos UTM9 を経由させる必要があります。その為、プライベートセグメントに展開したスイッチに保護対象を接続し、デフォルトゲートウェイを Sophos UTM9 に対し設定する必要があります。

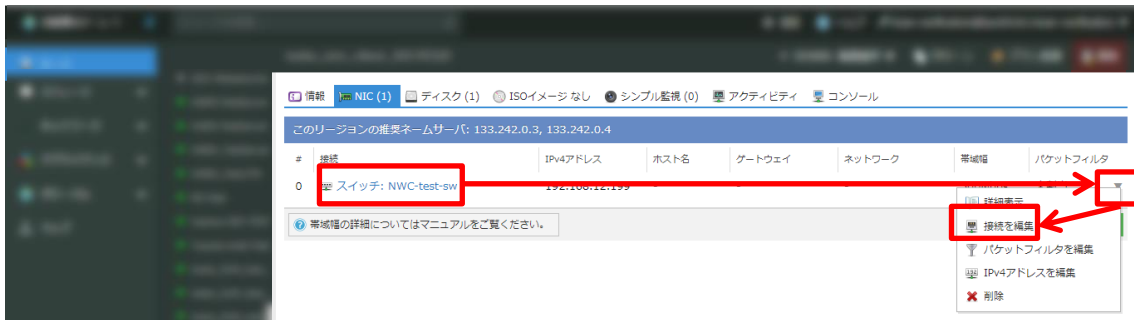
①保護対象システムをスイッチに接続するために、シャットダウンを実行します。

画面左下の Windows マークを押下し、電源マークからシャットダウンを押下します。

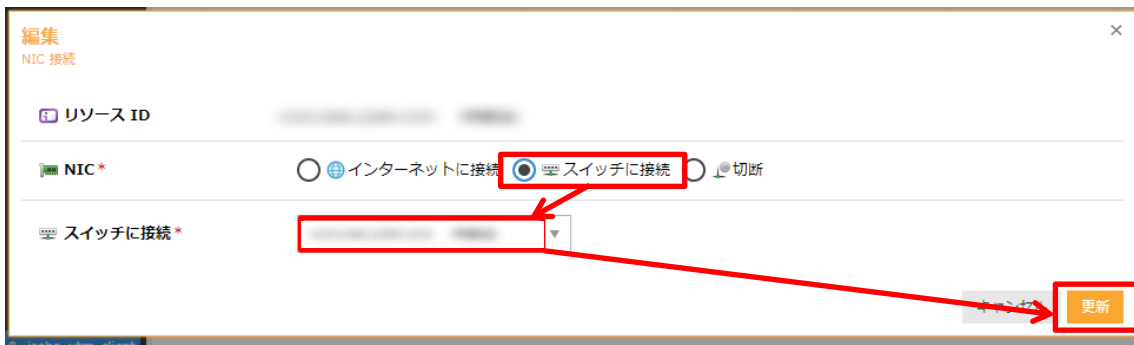


②NIC を作成したスイッチに接続します。

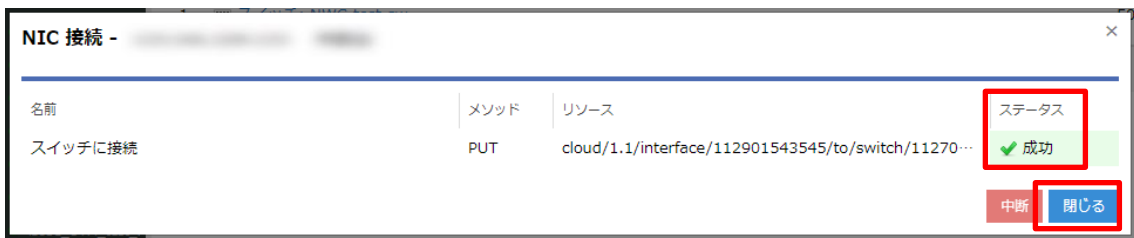
NIC 列の最右のメニューを展開し、接続を編集を押下します。



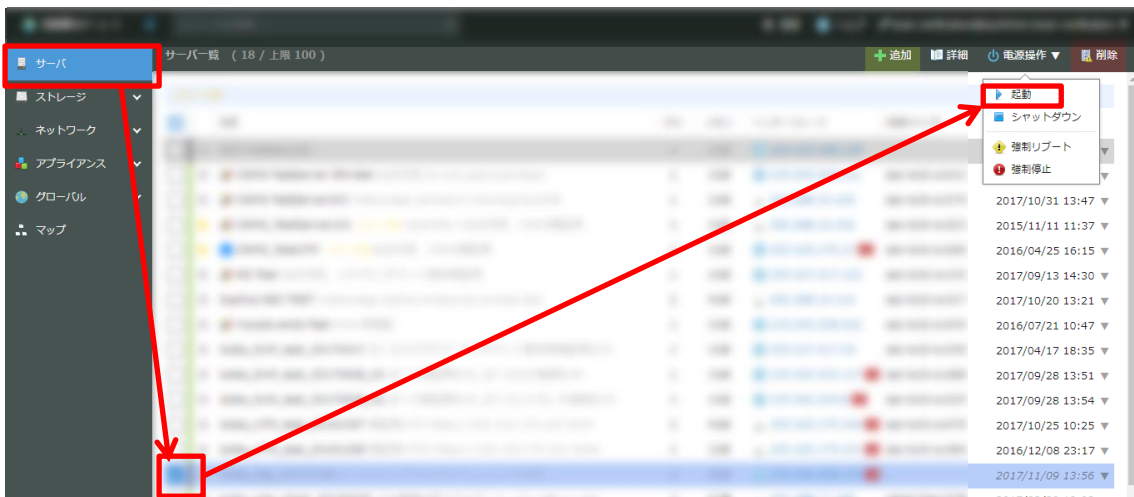
スイッチに接続を選択し、対象のスイッチを選択し更新を押下します。



NIC 接続プロセスが成功したことを確認します。



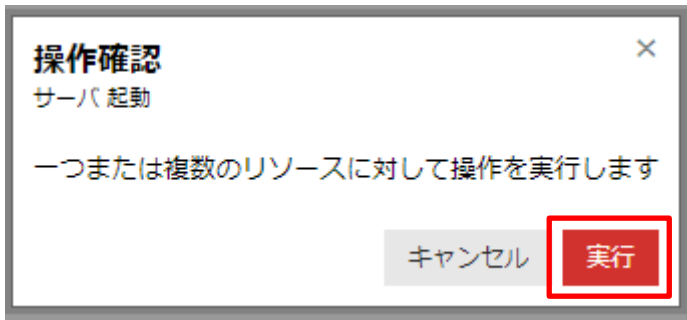
③さくらのクラウドコントロールパネルより保護対象システムのインスタンスの起動処理を行います。サーバメニューより、保護対象システムのインスタンスを選択し、電源操作 > 起動 を押下します。



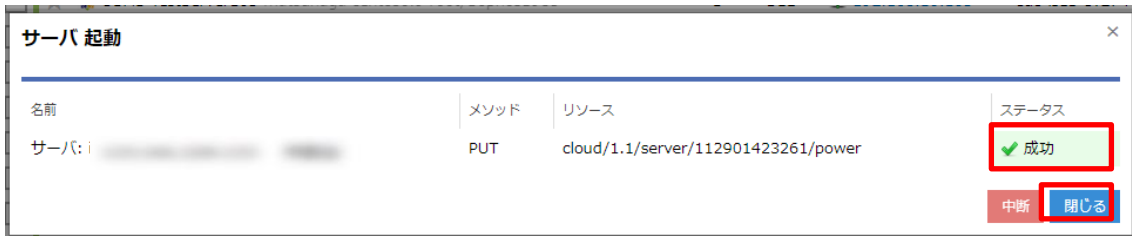
確認画面から、起動ボタンを押下します。



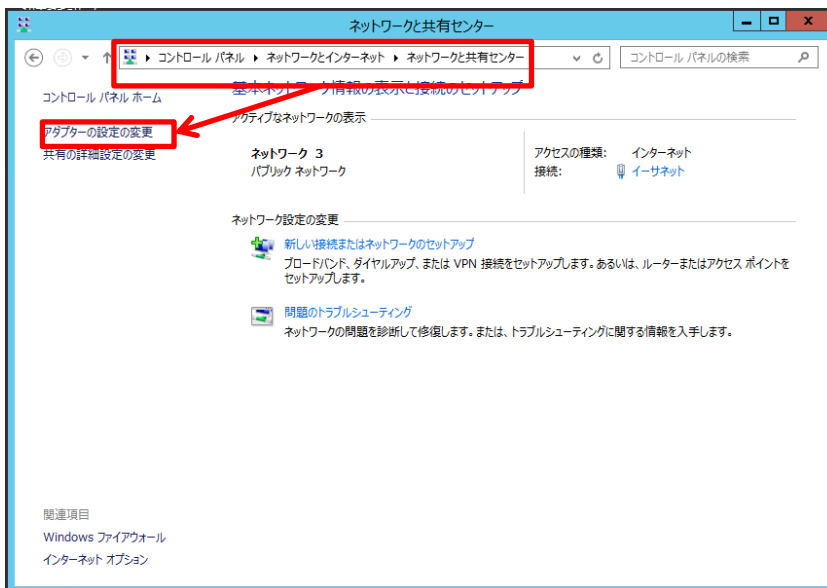
確認画面より実行ボタンを押下します。



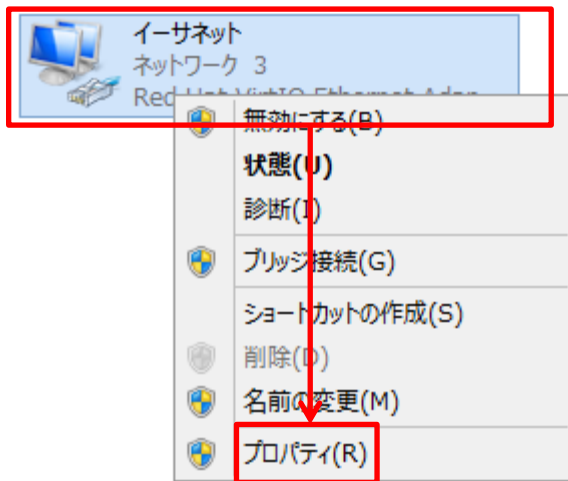
サーバ起動プロセスが成功したことを確認します。



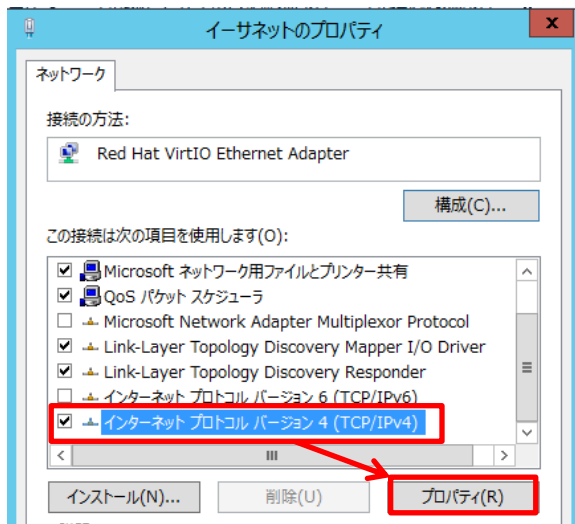
④保護対象システムへアクセスし IP アドレスとデフォルトゲートウェイの設定を行います。
コントロール パネル > ネットワークとインターネット > ネットワークと共有センター
を開き、アダプターの設定変更を押下します。



該当の NIC（アダプター）を右クリックしプロパティを押下します。

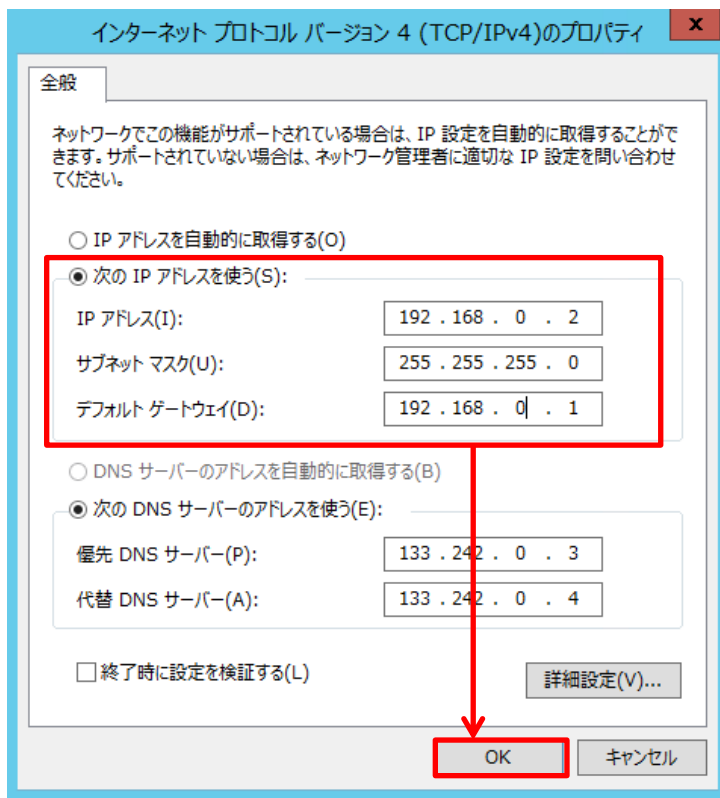


インターネットプロトコルバージョン 4（TCP/IP4）を選択し、プロパティを押下します。



プロパティ画面から以下の通り、設定を入力し、OK ボタンを押下します。

- 次の IP アドレスを使う：チェック
- IP アドレス：192.168.0.2
サブネットマスク：255.255.255.0
デフォルトゲートウェイ：192.168.0.1



プロパティ画面に戻るなので OK ボタンを押下し、アダプターの設定変更画面を閉じます。
以上で、保護対象システム（WindowsServer2012R2）の初期設定手順は完了です。