A10ネットワークス Thunderシリーズ ハンズオントレーニング

Ver.20220725

Reliable Security Always™

ハンズオントレーニング Agenda

（１）　ハンズオンの準備
- 時間　10分

（２）　ネットワークの設定
- 時間　40分（ハンズオン20分）

（３）　基本的なサーバ負荷分散の設定(L4 SLB)
- 時間　40分（ハンズオン20分）

（４）　アプリケーション負荷分散の設定(L7 SLB)
- 時間　30分（ハンズオン20分）

（５）　その他
- 時間　60分(付録紹介)

合計180分

（１）ハンズオンの準備

サーバ負荷分散の主な目的とコンセプト

（１）複数のサーバへ処理を分散 することによりサービス全体の処理能力をアップ

サーバ負荷分散

（２）サーバヘルスモニタによりサービスの可用性を高める

サーバヘルスモニタによるサービスの正常性チェック

ヘルスモニタによる
DOWN検知

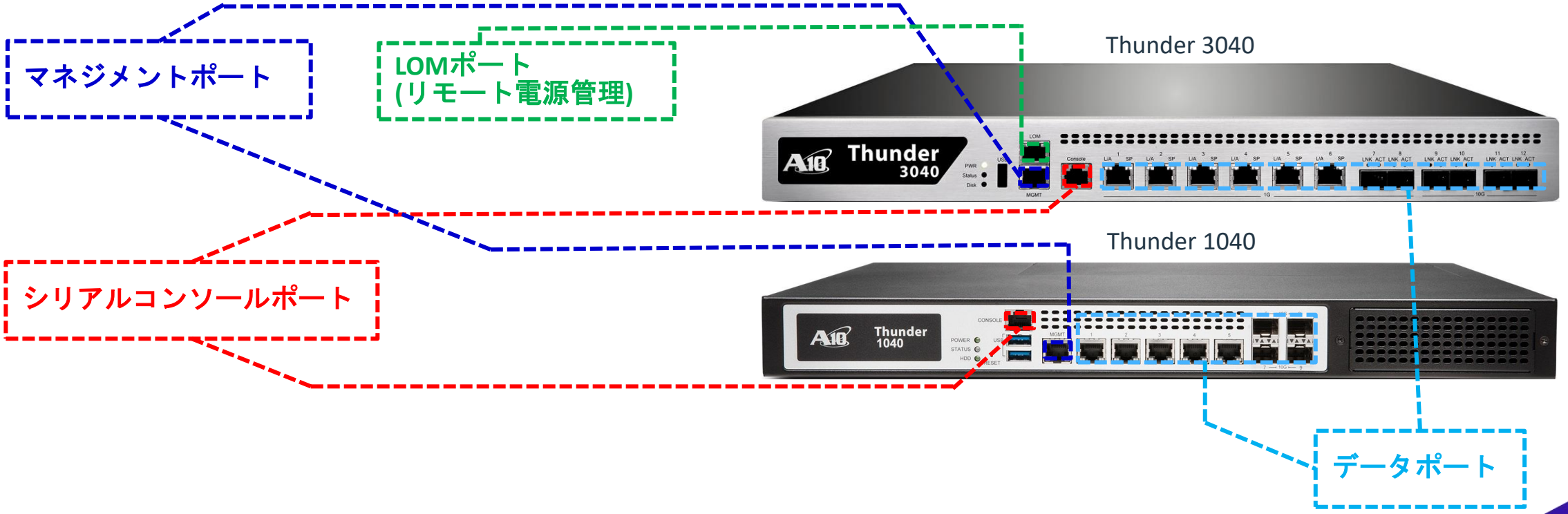
サーバ負荷分散装置が動作するレイヤ

- レイヤ４～７で動作します

7	アプリケーション層	サーバロードバランサー ***セッションベース***
6	プレゼンテーション層	
5	セッション層	
4	トランスポート層 TCP/UDP	
3	ネットワーク層 IP	L2/3スイッチ ***パケットベース***
2	データリンク層 Ethernet	
1	※OSI 7階層モデル　物理層	

Thunderの管理方法

- マネジメントポート
  ※Thunderには管理専用のマネジメントポートが搭載されています



Thunderの管理方法

操作インターフェイス

- **CLI（コマンドラインインターフェイス）**
  - シリアルコンソール接続 (RS-232 /9600 bps, 8 bit, N, 1bit / RJ45コネクタ)
  - TELNET接続(デフォルト無効)
  - SSH接続（SSH v2）
- **WEB GUI**
  - HTTP (HTTPSへリダイレクト)
  - HTTPS
- **デフォルトのアドレス設定(マネジメントインターフェイス)**
  172.31.31.31/24

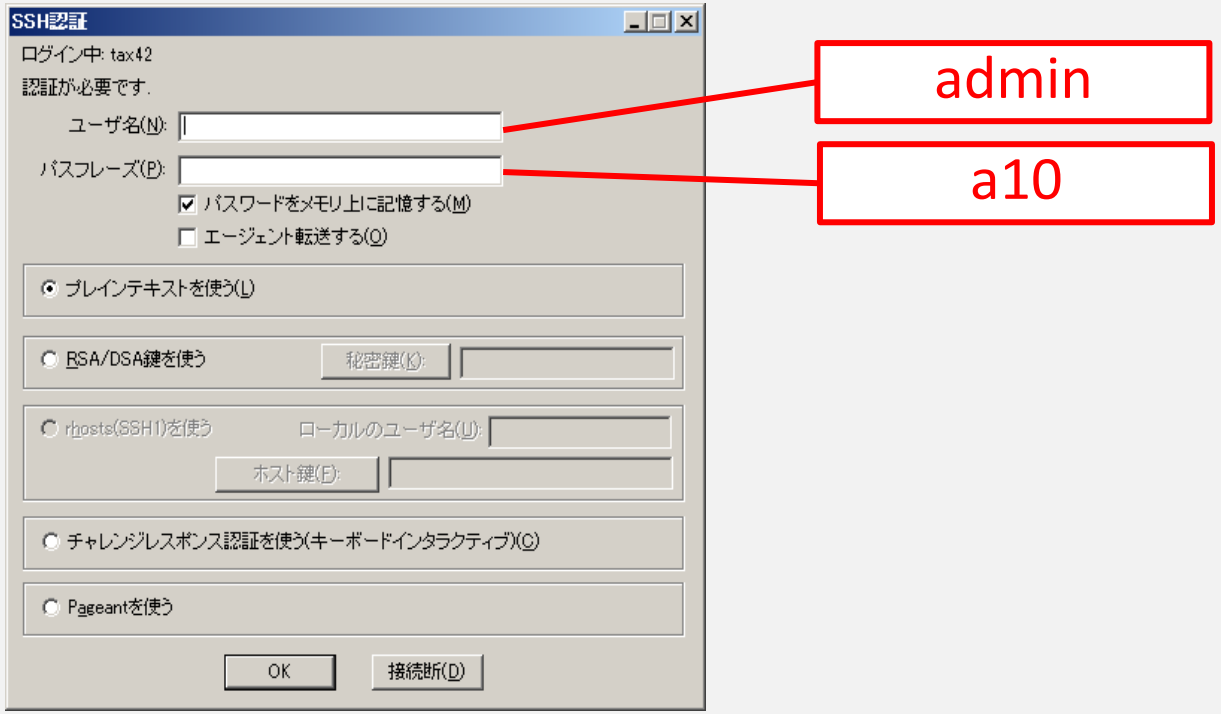
ログイン認証

- **ログインID/パスワード**
  - admin / a10 （デフォルト）
- **Enableパスワード（Enableモードへの移動時）**
  - パスワードなし（デフォルト）

Thunderの管理方法

デフォルトのログインアカウント

- ユーザ名： **admin**
- パスワード： **a10**
- Enableパスワード： **なし**

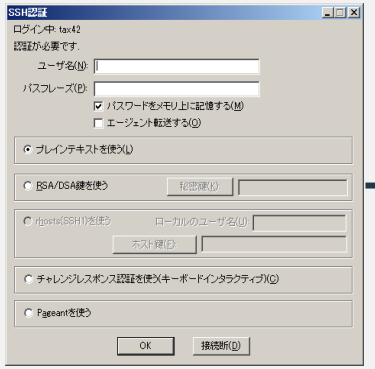


※TeratermによるSSHリモートログイン

Thunderの管理方法

CLIモード

- Execモード
- Enableモード
- Configモード



CLIログイン

Execモード

show コマンド
（config参照不可）
backup コマンド
Ping コマンド

Enableモード

show コマンド
（config参照可）
reboot/reload/shutdownコマンド

Configモード

設定変更を行う
コマンド等

CLI 基本コマンド

- **Enableモードへの移動**
  > enable

- **コンフィグモードへの移動**
  # config

- **設定したコンフィグの削除**
  # no <コマンド>

```
Last login: Sun Mar 15 21:40:35 2020 from 192.168.0.100

ACOS system is ready now.

[type ? for help]

vThunder>enable
Password: ⏎（リターン）
```

```
vThunder#config
vThunder(config)#
```

```
vThunder(config)#no vlan 10
```

CLI 基本コマンド

Thunderの設定の参照

show running-config

```
vThunder#show running-config
!Current configuration: 396 bytes       !Configuration last updated at 21:48:17
PDT Sun Mar 15 2020!Configuration last saved at 21:48:17 PDT Sun Mar 15
2020!64-bit Advanced Core OS (ACOS) version 4.1.4-GR1, build 78 (Jan-18-
2019,16:02)
!
interface management
  ip address 192.168.0.1 255.255.255.0
  ip default-gateway 192.168.0.254
!
interface ethernet 1
!
interface ethernet 2
:
```

（２） ネットワークの設定

コマンドラインインターフェイスによる設定
※WEB GUIインターフェイス設定も可能

２つのネットワーク動作モード

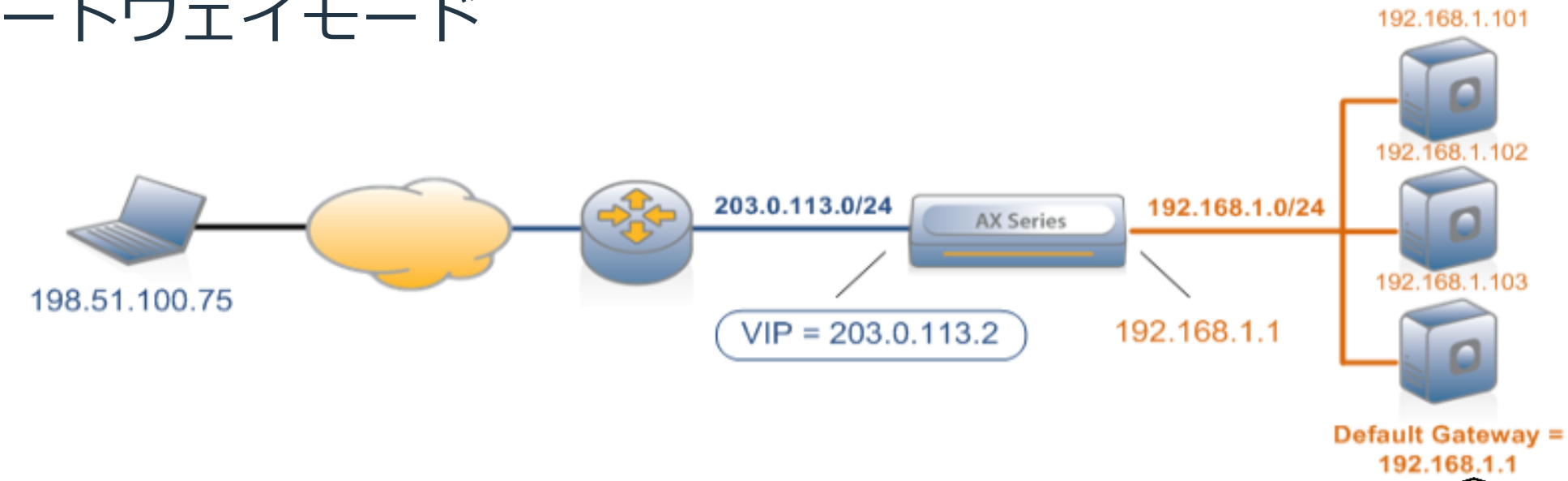
（１）ゲートウェイモード（デフォルト）
- L3（ルータ）として動作
- VE（VLANインターフェイス）の設定が可能
- IPフォワーディング（ルーティング）が可能

（２）トランスペアレントモード
- L2（スイッチ）として動作
- システムIPアドレスを設定
- VE設定、IPフォワーディングは不可

※2つのモードの切り替えにはreboot/reloadが必要

ネットワーク動作モード

（1）ゲートウェイモード



Client

Src IP	Dst IP
198.51.100.75	203.0.113.2

Thunder

Src IP	Dst IP
198.51.100.75	192.168.1.101

Server

Client

Dst IP	Src IP
198.51.100.75	203.0.113.2

Thunder

Dst IP	Src IP
198.51.100.75	192.168.1.101

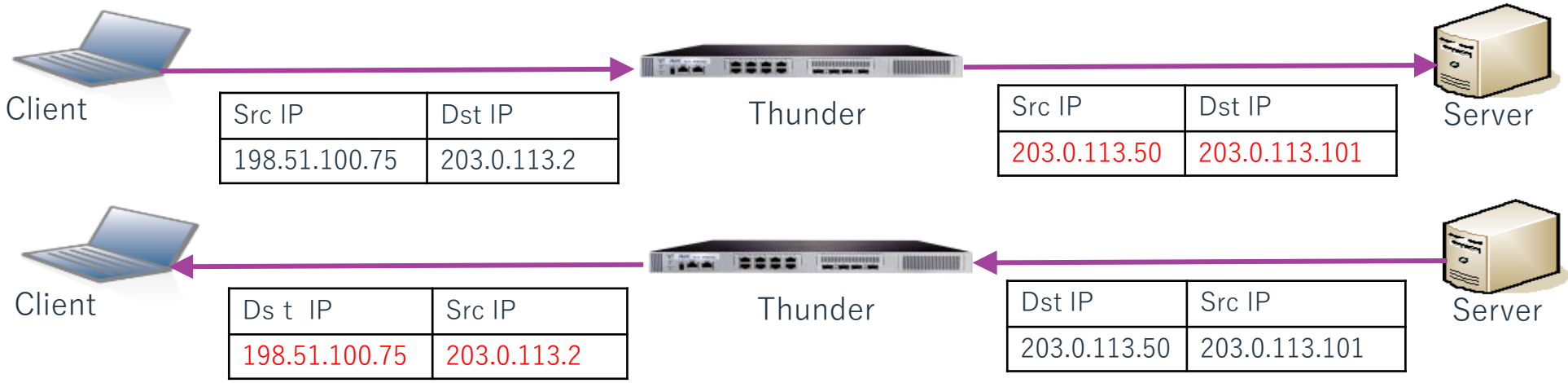
Server

ネットワーク動作モード

（1）ゲートウェイモード　SNATワンアーム構成

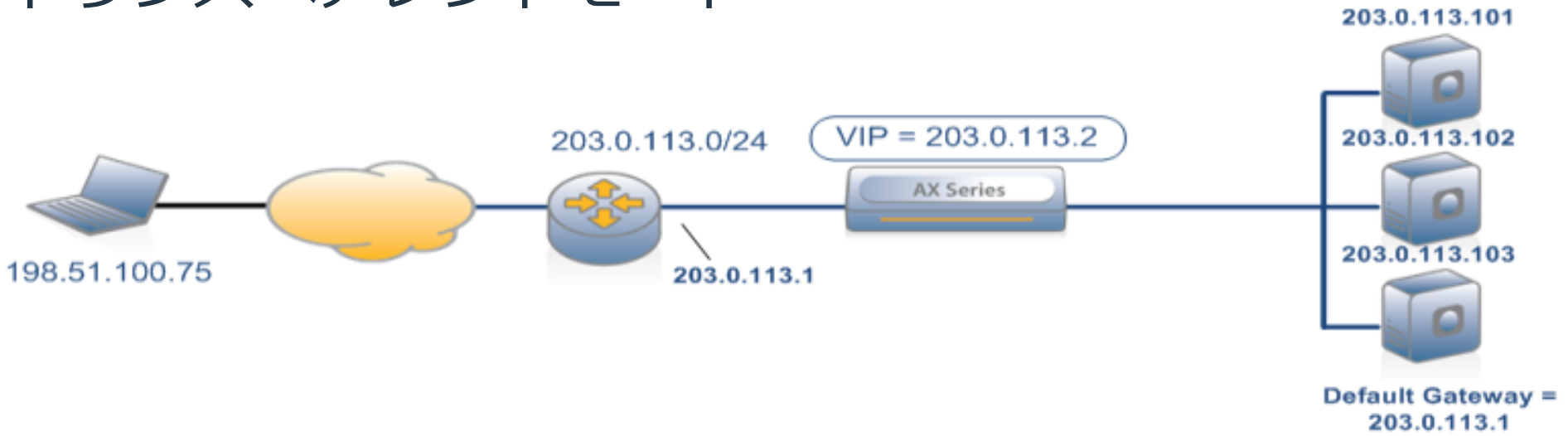
- SNAT: Source-NAT

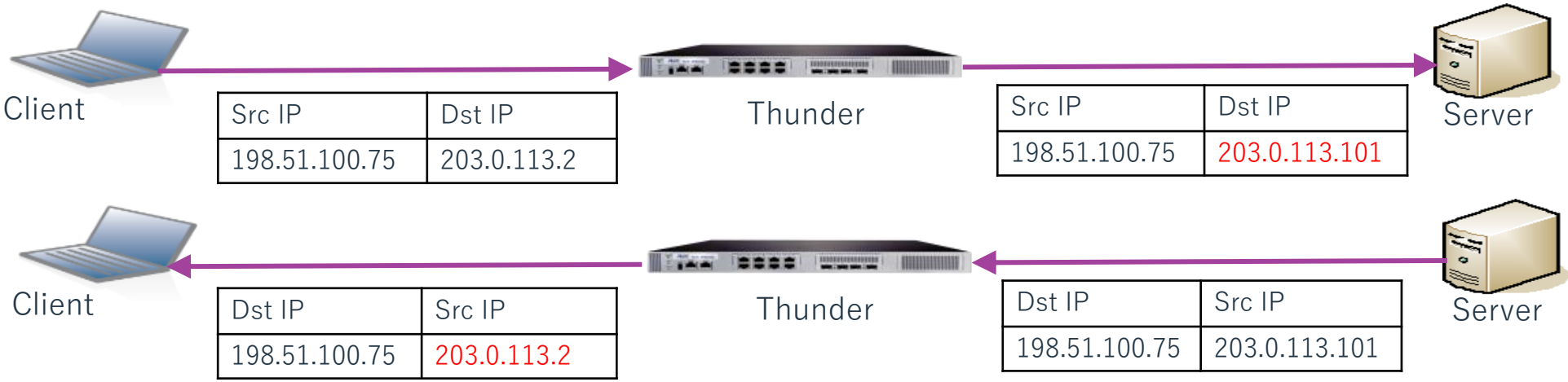
通常、上りと下り両方のトラフィックがA10を通るようにします。



ネットワーク動作モード

（2）トランスペアレントモード





インターフェイスの設定

- インターフェイスを有効(enable)に使用します。
- 最もシンプルな設定例:
  - (config)# **interface ethernet *[N]***
  - (config-if:ethernet:***N***) **ip address *A.B.C.D /nn***
  - (config-if:ethernet:***N***) **enable**

※N:ポート番号，/nn:サブネットマスク

[設定例]
(config)# **interface ethernet *3***
(config-if:ethernet:***N***) **ip address *1.1.1.1 /24***
(config-if:ethernet:***N***) **enable**
※3:ポート番号，/24:サブネットマスク

インターフェイスの設定(推奨)

VLANで柔軟に

- タグ付きまたはタグ無し（規格：IEEE802.1Q）
- ADP（A10の仮想機能）ではタグを使用し物理ポートを共有します。

推奨する設定例：

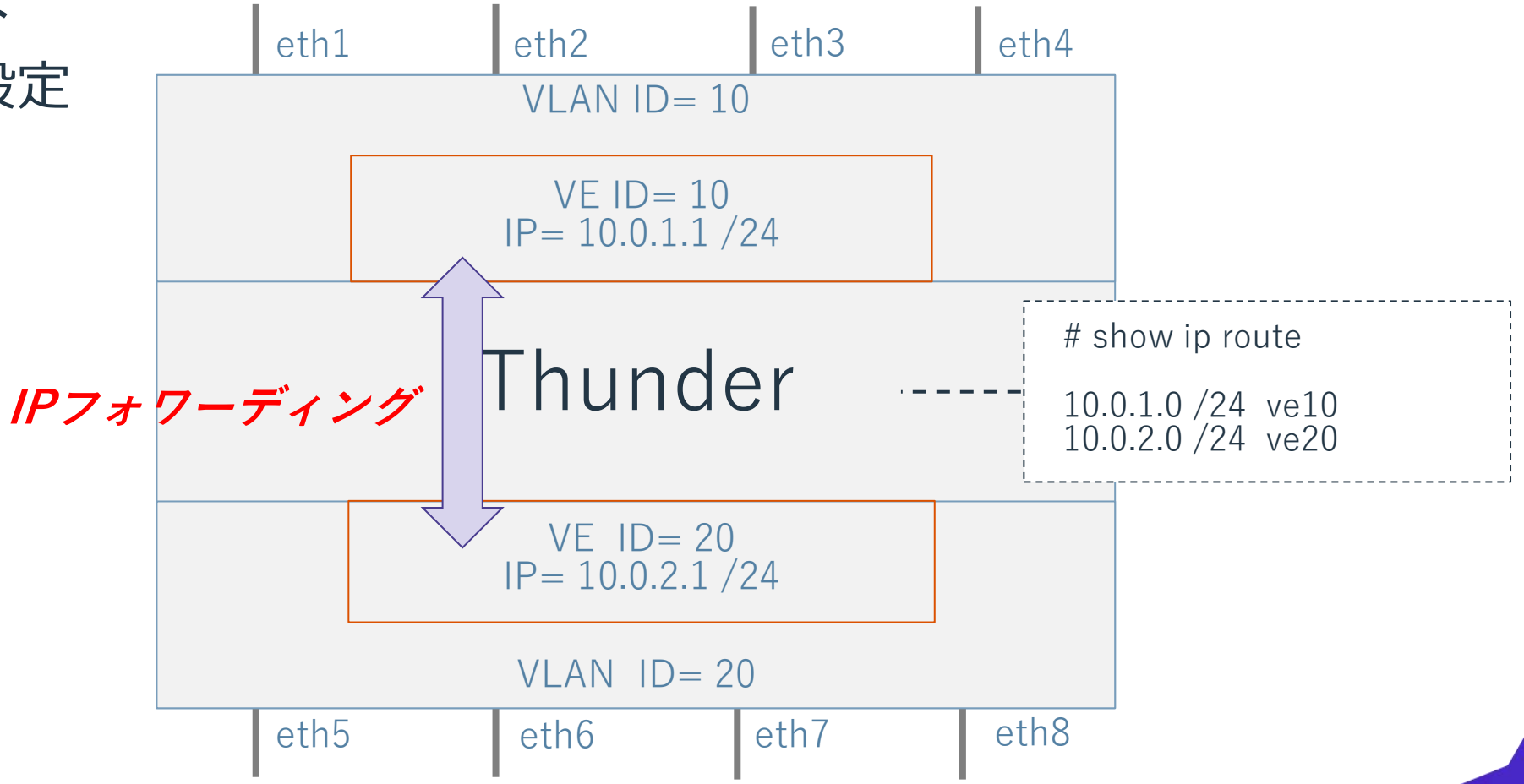
- (config)# **vlan *[N]***
- (config-vlan:*N*)# **[tagged|untagged] ethernet *[M]***
- (config-vlan:*N*)# **router-interface ve *[N]***
- (config)# **interface ve *[N]***
- (config-if:ve:*N*)# **ip address *<A.B.C.D>* /nn**
- **※N：VlanID，M：ポート番号，/nn：サブネットマスク**

[設定例]

```
(config)# vlan 10
(config-vlan:N)# tagged ethernet 3
(config-vlan:N)# router-interface ve 10
(config)# interface ve 10
(config-if:ve:N)# ip address 1.1.1.3 /24
```

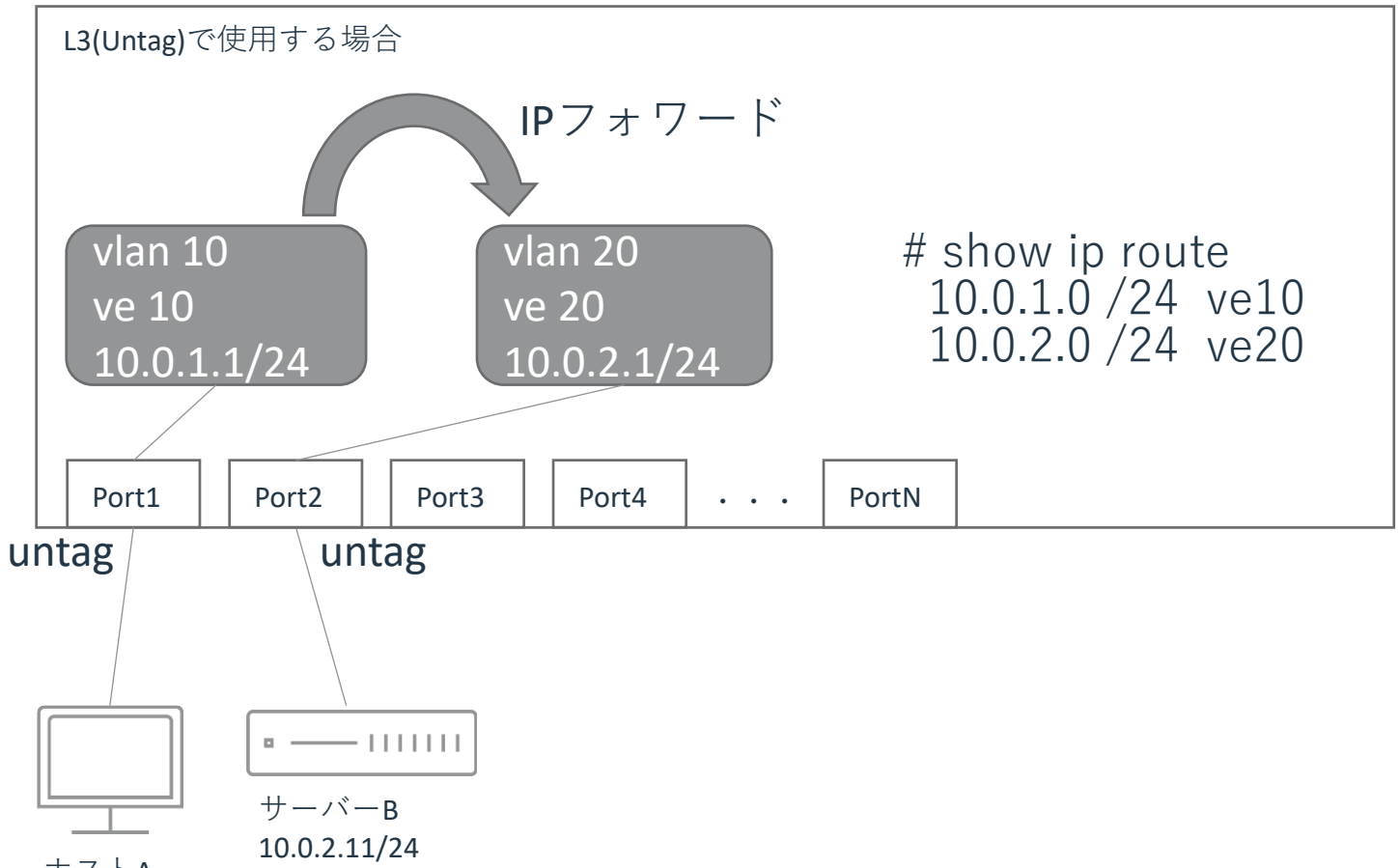
ネットワーク コンフィグデザイン

- Gatewayモード
  - ネットワーク設定
    - L2 /3 設定



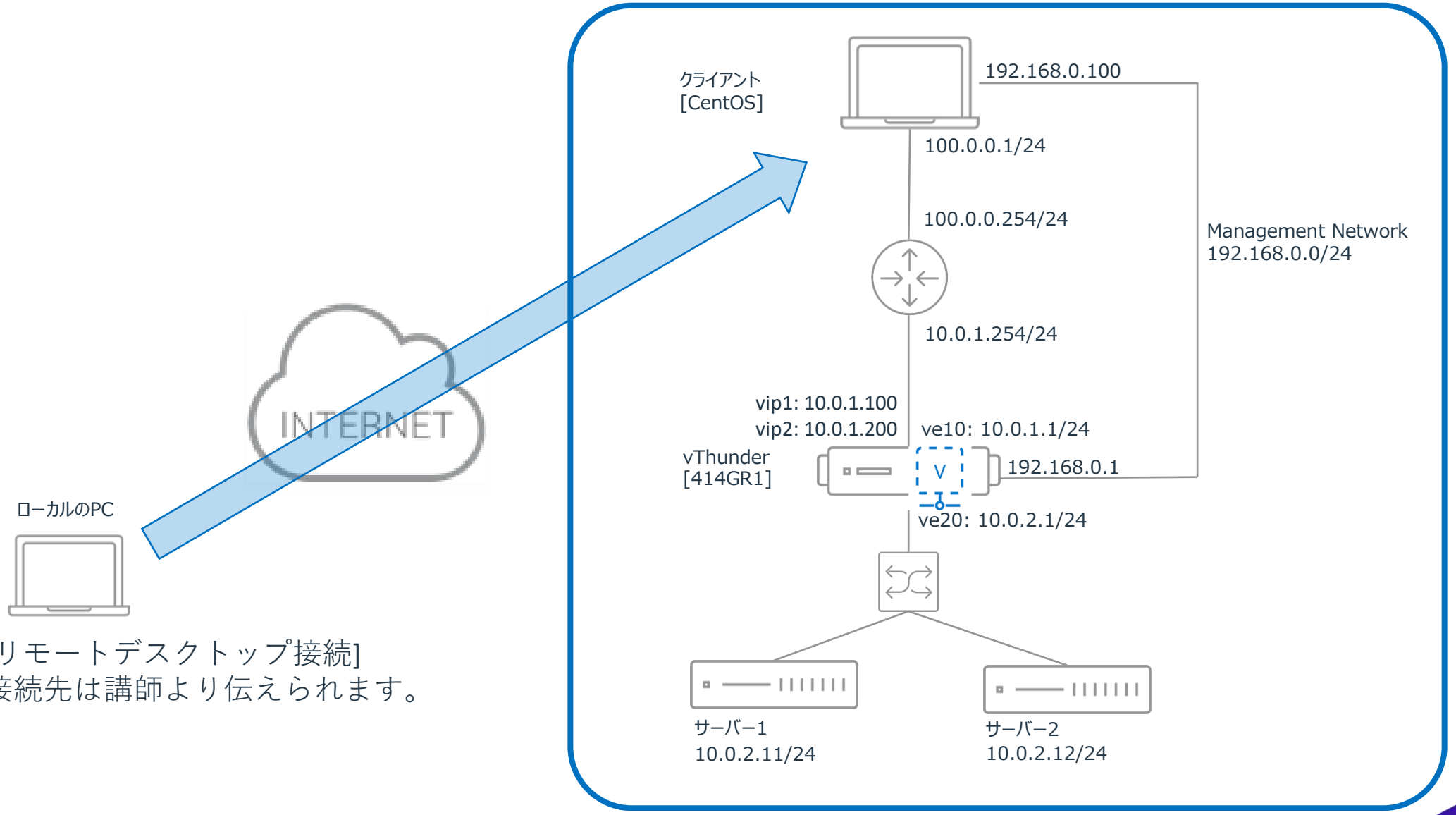
vlanインターフェイス(L3で使用する場合)

以下のように設定します。




```
A10(config)#vlan 10
A10(config-vlan:10)#untagged ethernet 1
A10(config-vlan:10)#router-interface ve 10
A10(config)#interface ve 10
A10(config-if:ve:10)#ip address 10.0.1.1 /24
A10(config)#
A10(config)#vlan 20
A10(config-vlan:10)#untagged ethernet 2
A10(config-vlan:10)#router-interface ve 20
A10(config)#interface ve 20
A10(config-if:ve:10)#ip address 10.0.2.1 /24
```

ラボネットワーク構成



[リモートデスクトップ接続]
接続先は講師より伝えられます。

ラボ（１）環境設定

- VLAN / Ethernet Interface / VE interface 割り当て

Thunder	VLAN 10	VLAN 20
A10	Ethernet **1** VE 10	Ethernet **2** VE 20

ラボ（１）環境設定

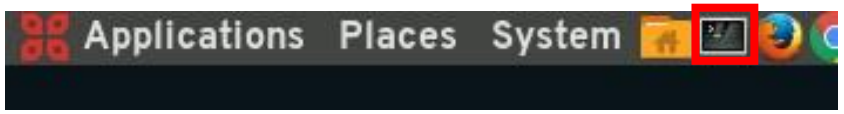
- アドレス割り当て

Thunder	VE 10	VE 20	Default Gateway
A10	10.0.1.1 /24	10.0.2.1 /24	10.0.1.254

ラボ（１）ゲートウェイモード　ネットワーク設定

Terminal起動

DesktopのTerminalアイコンをクリックして起動してください。



「192.168.0.1」へのログイン

Terminalの接続先ホストとして「 192.168.0.1 」を指定して、SSHログインしてください

ユーザID: admin パスワード: a10

$ssh admin@192.168.0.1⏎（リターン）

Password: a10⏎（リターン）

Enableモードへ移動します

> enable

Password: ⏎（リターン）

Configモードへ移動します

config

ラボ（1）ゲートウェイモード　ネットワーク設定

Hostnameの設定

hostname <name>

```
vThunder(config)#hostname A10
A10(config)#
```

VLANの作成

vlan <num>
untagged ethernet <num>
router-interface ve <num>

※vlan 10, 20 を作成します

```
A10(config)#vlan 10
A10(config-vlan:10)#untagged ethernet 1
A10(config-vlan:10)#router-interface ve 10
A10(config)#
A10(config)#vlan 20
A10(config-vlan:10)#untagged ethernet 2
A10(config-vlan:10)#router-interface ve 20
```

ラボ（1）ゲートウェイモード　ネットワーク設定

Interfaceのenable

出荷状態がdisableのためenableが必要
interface ethernet <num>
enable
※ethernet 1, 2 の設定を行います

```
A10(config)#interface ethernet 1
A10config-if:ethernet:1)#enable

A10(config)#interface ethernet 2
A10config-if:ethernet:1)#enable
```

VEの設定

interface ve <num>
ip address <address> <netmask>
※ve 10, 20　の設定を行います

```
A10(config)#interface ve 10
A10(config-if:ve:10)#ip address 10.0.1.1 /24

A10(config)#interface ve 20
A10(config-if:ve:10)#ip address 10.0.2.1 /24
```

デフォルトゲートウェイの設定

ip route 0.0.0.0 /0 <gateway address>

```
A10(config)#ip route 0.0.0.0 /0 10.0.1.254
```

ラボ（1）ゲートウェイモード　ネットワーク設定

設定の確認

インターフェイスのLinkUp

show interface brief

```
A10#show interfaces brief
Port    Link  Dupl  Speed  Trunk Vlan MAC           IP Address        IPs  Name
-----------------------------------------------------------------------------------
mgmt    Up    auto  auto   N/A   N/A  2cc2.607b.00a1  192.168.0.1/24      1
1       Up    Full  10000  none  10   2cc2.607b.10a1  0.0.0.0/0           0
2       Up    Full  10000  none  20   2cc2.607b.20a1  0.0.0.0/0           0
3       Disb  None  None   none  1    2cc2.607b.30a1  0.0.0.0/0           0
```

VLANの確認

show vlans

※vlans　複数形で指定

```
A10#show vlans
Total VLANs: 3
:
VLAN 10, Name [None]:
 Untagged Ethernet Ports: 1
  Tagged Ethernet Ports: None
:
      Router Interface: ve 10

VLAN 20, Name [None]:
 Untagged Ethernet Ports: 2
:
      Router Interface: ve 20
```

ラボ（１）ゲートウェイモード　ネットワーク設定

設定の確認

VE IPの確認

show ip interfaces ve

```
A10# show ip interfaces ve
Port    IP          Netmask       PrimaryIP   Name
-------------------------------------------------------
ve10    10.0.1.1    255.255.255.0   Yes
ve20    10.0.2.1    255.255.255.0   Yes
```

ルーティングテーブルの確認

show ip route

```
A10#show ip route
:
* - candidate default

Gateway of last resort is 10.0.1.1 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 10.0.1.254, ve 10
C       10.0.1.0/24 is directly connected, ve 10
C       10.0.2.0/24 is directly connected, ve 20
```

ラボ（1）ゲートウェイモード・ネットワーク設定

動作確認

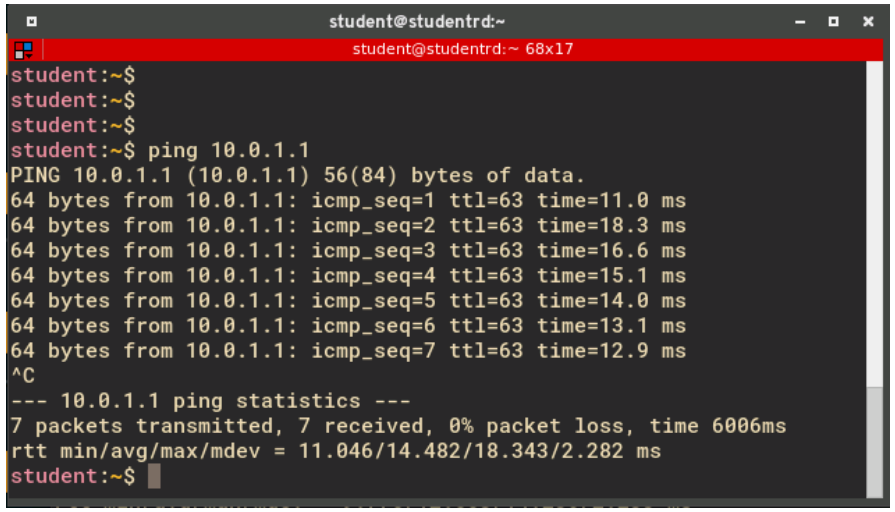
- A10 ThunderからDefault Gateway 10.0.1.254 へのPing確認

  # ping 10.0.1.254

- A10 ThunderからServer 10.0.2.11 へのPing確認

  # ping 10.0.2.11

- DesktopのTerminalから10.0.1.1のIPへPing確認



ラボ（1）ゲートウェイモード　ネットワーク設定

- サンプルコンフィグ

```
hostname A10
!
vlan 10
  untagged ethernet 1
  router-interface ve 10
!
vlan 20
  untagged ethernet 2
  router-interface ve 20

interface ethernet 1
  enable
!
interface ethernet 2
  enable
!
interface ve 10
  ip address 10.0.1.1 255.255.255.0
!
interface ve 20
  ip address 10.0.2.1 255.255.255.0
!
!
ip route 0.0.0.0 /0 10.0.1.254
!
```

CLI：コンフィグのインデント

[コンフィグ例]

```
slb virtual-server vip2 10.0.1.200
   port 80 http
      service-group sg-80
```

```
A10#configure
A10(config)#slb virtual-server vip2
A10(config-slb vserver)#port 80 http
A10(config-slb vserver-vport)#service-group sg-80
A10(config-slb vserver-vport)#exit
A10(config-slb vserver)#exit
A10(config)#exit
A10#
```

Ctrl-CはconfigモードのexitのキーボードショートカットCtrl-Zはconfigモードのendのキーボードショートカット

```
A10#configure
A10(config)#slb virtual-server vip2
A10(config-slb vserver)#port 80 http
A10(config-slb vserver-vport)#service-group sg-80
A10(config-slb vserver-vport)#end
A10#
```

CLI：ヘルプ

- リストオプション
  - ACOS> **show health monitor ?**
  - WORD<length:1-31> Name
    all-partitions All partition configurations
    partition Per-partition configurations
    | Output modifiers
- オプションの曖昧さ回避
  - ACOS> **show ic?**
  - icmp Display ICMP statistics
    icmpv6 Display ICMPv6 statistics
- コマンドの完了
  - ACOS> **show rad*<tab>***
    ACOS> show radius-server
- コマンドの連続実行
  - ACOS> **repeat 1** show cpu //1秒に一回実行
    ACOS> **repeat 5** show interfaces statistics //5秒に一回実行

CLI:設定の初期化

- マネジメントIP設定を残してコンフィグを初期化

A10(config)#erase preserve-management reload
Please confirm: Erase startup configuration (Y/N)?: y
System has reloaded successfully.

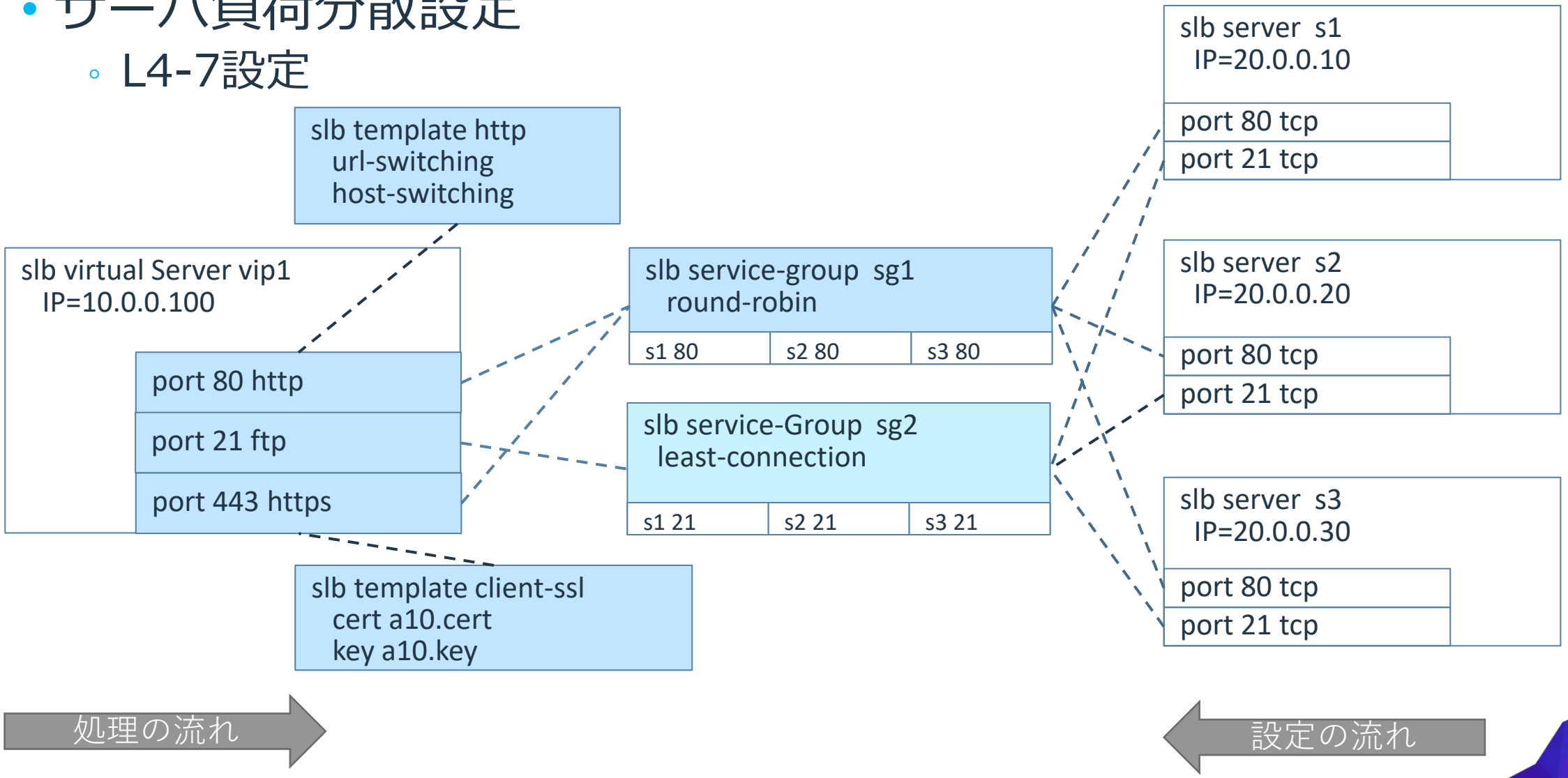
※本ラボでは実行しません。

（３） 基本的なサーバ負荷分散

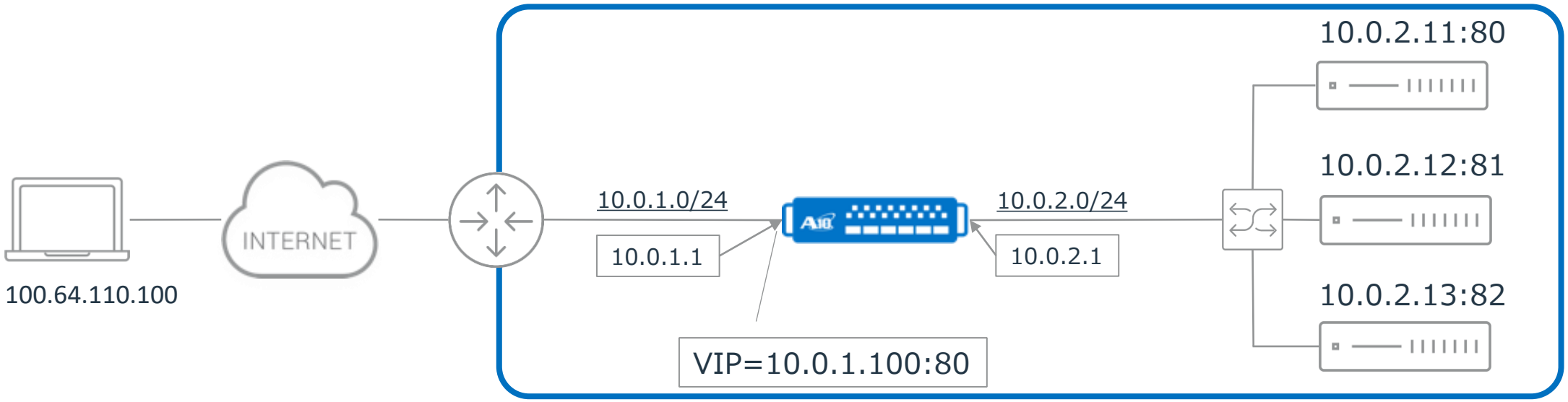
コマンドラインインターフェイスによる設定
※WEB GUIインターフェイス設定も可能

コンフィグデザイン

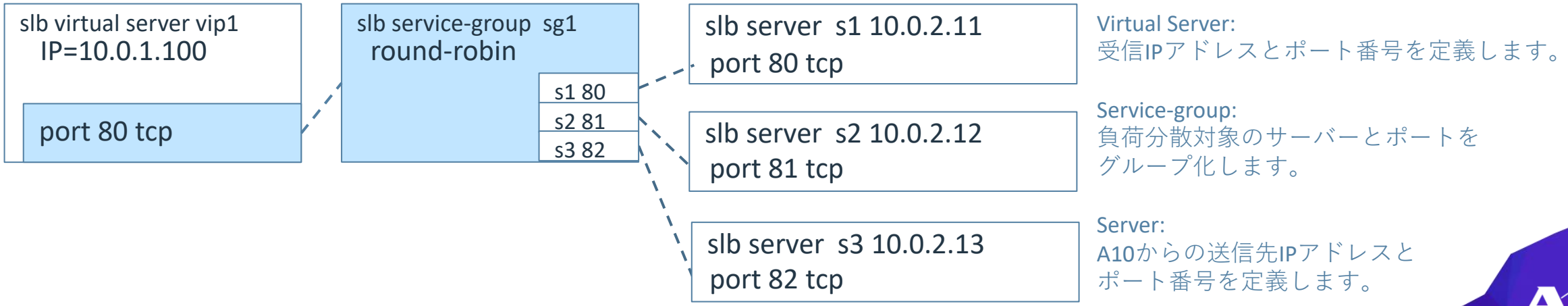
- サーバ負荷分散設定
  - L4-7設定



ロードバランサーの基本構成



Thunderの設定



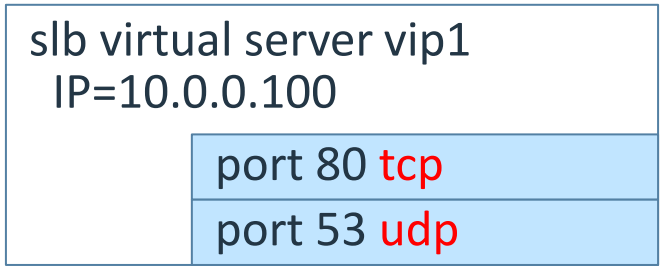
Virtual Server:
受信IPアドレスとポート番号を定義します。

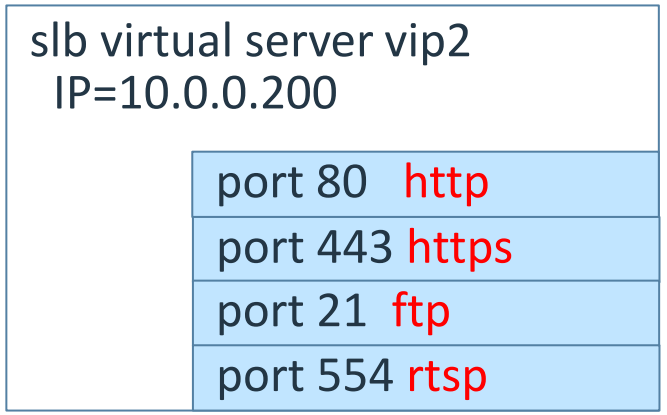
Service-group:
負荷分散対象のサーバーとポートを
グループ化します。

Server:
A10からの送信先IPアドレスと
ポート番号を定義します。

バーチャルサーバ サービスタイプ

- サービスタイプ
  - Thunderの仮想サービス（Virtual Server）のPortの動作を設定します
  - レイヤ4サービスタイプ
    - TCP
    - UDP
  - レイヤ7サービスタイプ
    - HTTP
    - HTTPS
    - FTP
    - RTSP/MMS
    - SMTP
    - SSL-Proxy
    - SIP





バーチャルサーバ サービスタイプ

- レイヤ4サーバ負荷分散（L4 SLB）

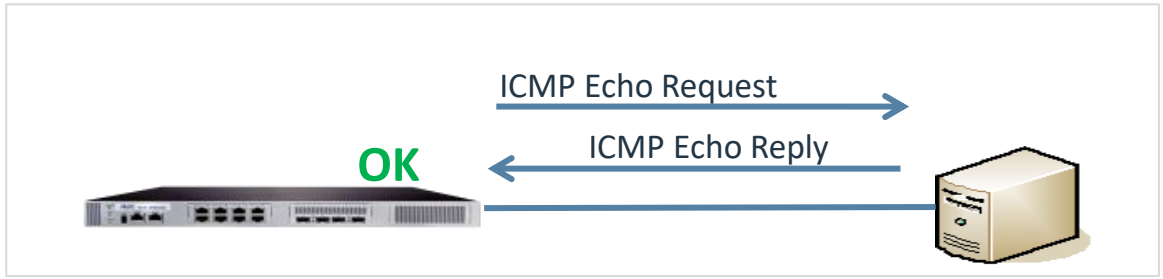
TCP	TCPレイヤ4負荷分散
UDP	UDPレイヤ4負荷分散

- レイヤ7サーバ負荷分散（L7 SLB）

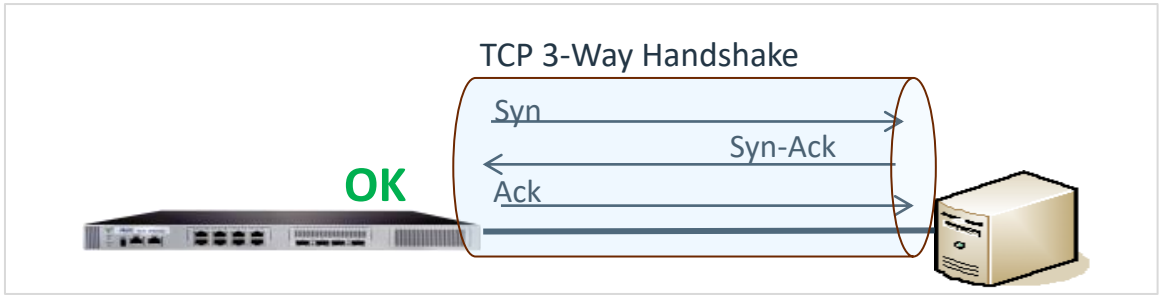
HTTP	HTTPアプリケーションレイヤ負荷分散
HTTPS	SSLアクセラレーション＋HTTP
FTP	FTPアプリケーションレイヤゲートウェイ
RTSP/MMS	ストリーミングプロトコル（RTSP/MMS）負荷分散
SMTP	SMTPアプリケーションレイヤ負荷分散
SSL-Proxy	SSLアクセラレーション＋レイヤ４負荷分散（LDAP/SMTP/POP3/IMAP）
SIP	SIPアプリケーションレイヤゲートウェイ

ヘルスモニタ

- レイヤ3ヘルスモニタ
  - ICMP(Ping)
  - サーバ作成時に自動的に有効



- レイヤ4ヘルスモニタ
  - tcp / udp
  - サーバポート設定時に自動的に有効

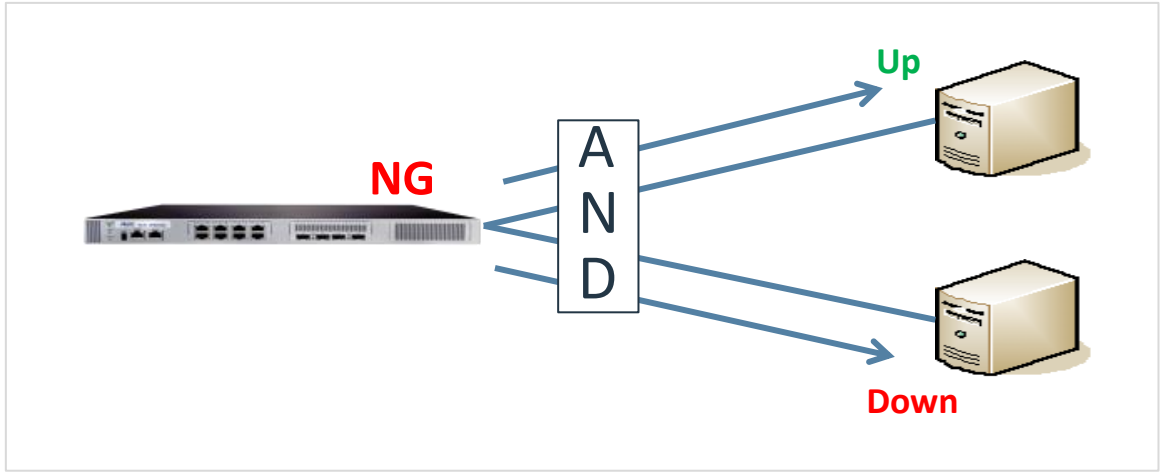


- レイヤ7ヘルスモニタ
  - http / https / ftp / smtp / pop3 / snmp / dns / radius / ldap / rtsp / sip / ntp
  - それぞれのアプリケーションレイヤでのチェック

ヘルスモニタ

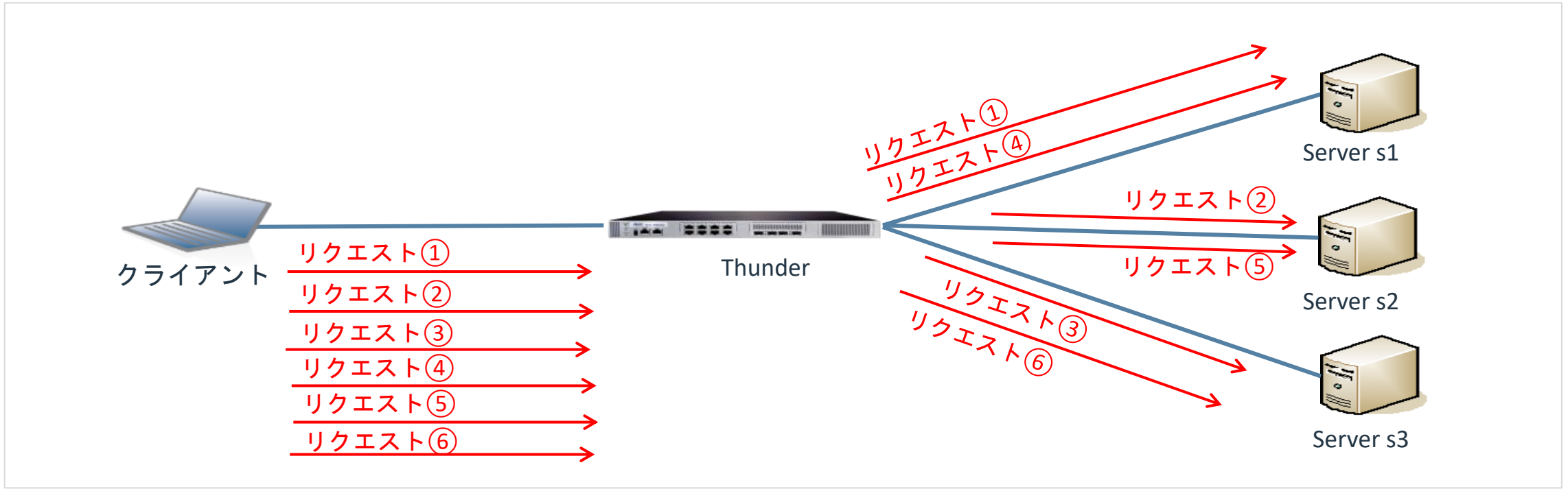
- カスタムヘルスモニタ
  - shell / perl / python / tcl
  - ユーザ定義のスクリプトによるヘルスチェック

- コンパウンド　ヘルスモニタ
  - 複数のレイヤ3 / レイヤ4 / レイヤ7レベルのヘルスモニタを論理式(and / or / not)で組み合わせ複合評価を行う



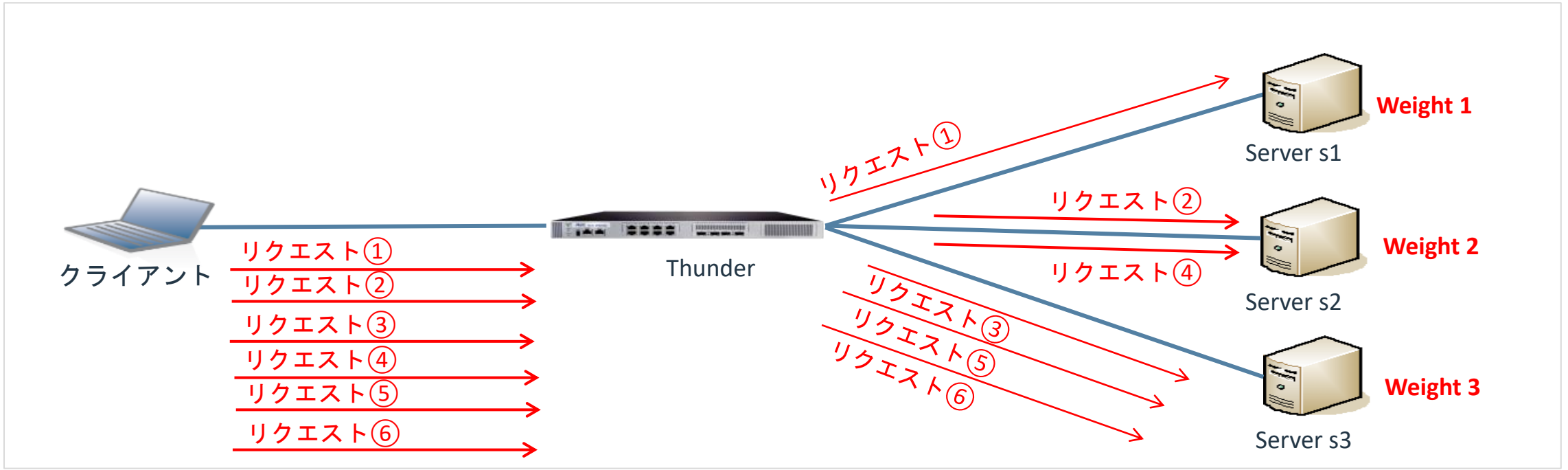
ロードバランシングアルゴリズム

- Round-Robin（デフォルト）
  - ラウンドロビン



ロードバランシングアルゴリズム

- Weighted Round-Robin
  - 静的に重み付けしたラウンドロビン



ロードバランシングアルゴリズム

- Least Connection
  - Server 単位で最少 Current Connectionのサーバを選択
  - 同一の場合にはリクエスト / レスポンスパケットの少ないサーバを選択

VIP	Port	Server s1	Server s2
10.0.1.100	port 80	15	20
	port 443	5	2
	合計	20	22

port 80の負荷分散 ⇒ Server s1
port 443の負荷分散 ⇒ Server s1

ロードバランシングアルゴリズム

- Service Least Connection
  - Service Port 単位で最小 Current Connectionのサーバを選択
  - 同一の場合にはリクエスト / レスポンスパケットの少ないサーバを選択

VIP	Port	Server s1	Server s2
10.0.1.100	port 80	15	20
	port 443	5	2

port 80の負荷分散 ⇒ Server s1
port 443の負荷分散 ⇒ Server s2

ラボ（２）環境設定

- Server IP / Virtual Server IPアドレス割り当て

Thunder	Server s1	Server s2	Virtual-Server vip1
A10	10.0.2.11	10.0.2.12	10.0.1.100

ラボ（２）基本サーバロードバランシング設定

1. Serverの設定

slb server s1 <address>
port 80 tcp
slb server s2 <address>
port 80 tcp

```
A10(config)# slb server s1  10.0.2.11
A10(config-real server) # port 80 tcp

A10(config)# slb server s2  10.0.2.12
A10(config-real server) # port 80 tcp
```

2. Service-Groupの設定

slb service-group sg-80 tcp
method service-least-connection
member s1 80
member s2 80

※methodコマンドは、ロードバランシングアルゴリズムが round-robin の時は設定不要です（デフォルト）

```
A10(config)# slb service-group sg-80 tcp
A10(config-slb svc group) # method service-least-connection
A10(config-slb svc group) # member s1 80
A10(config-slb svc group) # member s2 80
```

ラボ（２）基本サーバロードバランシング設定

3. Virtual Serverの設定

slb virtual-server vip1 <address>
port 80 tcp
service-group sg-80

```
A10(config)# slb virtual-server vip1 10.0.1.100
A10(config-slb vserver)# port 80 tcp
A10(config-slb vserver-vport)#service-group sg-80
```

ラボ（２）基本サーバロードバランシング設定

4. 設定の確認

#show runninig-config slb server

- Serverの設定確認

#show runninig-config slb service-group

- Service-groupの設定確認

#show runninig-config slb virtual-server

- Virtual-serverの設定確認

```
A10#show  running-config  slb server
slb server s1 10.0.2.11
   port 80  tcp
slb server s2 10.0.2.12
   port 80  tcp
```

```
A10#show  running-config  slb  service-group
slb service-group sg-80 tcp
    method service-least-connection
    member s1 80
    member s2 80
```

```
A10#sh running-config slb virtual-server
slb virtual-server vip1 10.0.1.100
   port 80  tcp
      service-group sg-80
```

ラボ（２）基本サーバロードバランシング設定

4. 設定の確認

- Serverステータスの確認

#show slb server

```
A10#show  slb  server
Total Number of Servers configured: 2
Total Number of Services configured: 2
              Current = Current Connections, Total = Total Connections
              Fwd-pkt = Forward packets, Rev-pkt = Reverse packets
Service              Current    Total     Fwd-pkt    Rev-pkt    Peak-conn  State
--------------------------------------------------------------------------------
s1:80/tcp            0          61256     173080     59327      0          Up
s1: Total            0          61256     173080     59327      0          Up

s2:80/tcp            1          61385     173365     59318      0          Up
s2: Total            1          61385     173365     59318      0          Up
```

現在のActiveなConnection

ヘルスチェックステータス

ラボ（２）基本サーバロードバランシング設定

4. 設定の確認

- ヘルスモニタステータスの確認

#show health stat

```
A10#show health stat
Health monitor statistics
:
:
IP address       Port  Health monitor  Status   Cause(Up/Down)  Reason(Up/Down)              Retry   Pin
-----------------------------------------------------------------------------------------------------
10.0.2.11              default          UP      11 /0  @0       ICMP Receive OK              0       0     /0  0
10.0.2.11        80    default          UP      20 /0  @0       TCP Verify Connection OK     0       0     /0  0
10.0.2.12              default          UP      11 /0  @0       ICMP Receive OK              0       0     /0  0
10.0.2.12        80    default          UP      20 /0  @0       TCP Verify Connection OK     0       0     /0  0
```

ヘルスモニタの実行結果

ヘルスモニタが実行されるサーバのポート番号
番号がないものはサーバのノード（IPアドレス）に対するヘルスモニタ(ICMP)

適用されているヘルスモニタ名。
defaultはデフォルトのヘルスモニタ

ラボ（２）基本サーバロードバランシング設定

4. 設定の確認

- セッションエントリの確認

#show session

```
A10#show session
:
:
Prot Forward Source       Forward Dest       Reverse Source     Reverse Dest          Age  Hash Flags    Type
-----------------------------------------------------------------------------------------------------------
Tcp  10.200.5.180:34704   10.0.1.111:80      10.0.2.18:80       10.200.5.180:34704    120  1    NFe0f0r0 SLB-L4
Tcp  10.200.5.180:34702   10.0.1.111:80      10.0.2.19:80       10.200.5.180:34702    120  1    NFe0f0r0 SLB-L4
Tcp  10.200.5.180:34706   10.0.1.111:80      10.0.2.18:80       10.200.5.180:34706    120  1    NFe0f0r0 SLB-L4
Total Sessions:       3
```

ラボ（２）基本サーバロードバランシング設定

4. 設定の確認

- 負荷分散パフォーマンス（CPS）の確認

#show slb performance

```
A10#show slb performance
Refreshing SLB performance every 1 seconds. (press ^C to quit)
Note: cpi conn/interval, tpi transactions/interval

CPU Usage       L4cpi   L7cpi   L7tpi   SSLcpi  ServSSLcpi  Natcpi  FWcpi   Time
-------------------------------------------------------------------------------
12/5/5/         60      0       0       0       0           0       0       19:03:20
```

新規L4コネクション/秒

新規L7 コネクション/秒

新規L7 リクエスト/秒

新規SSLコネクション/秒

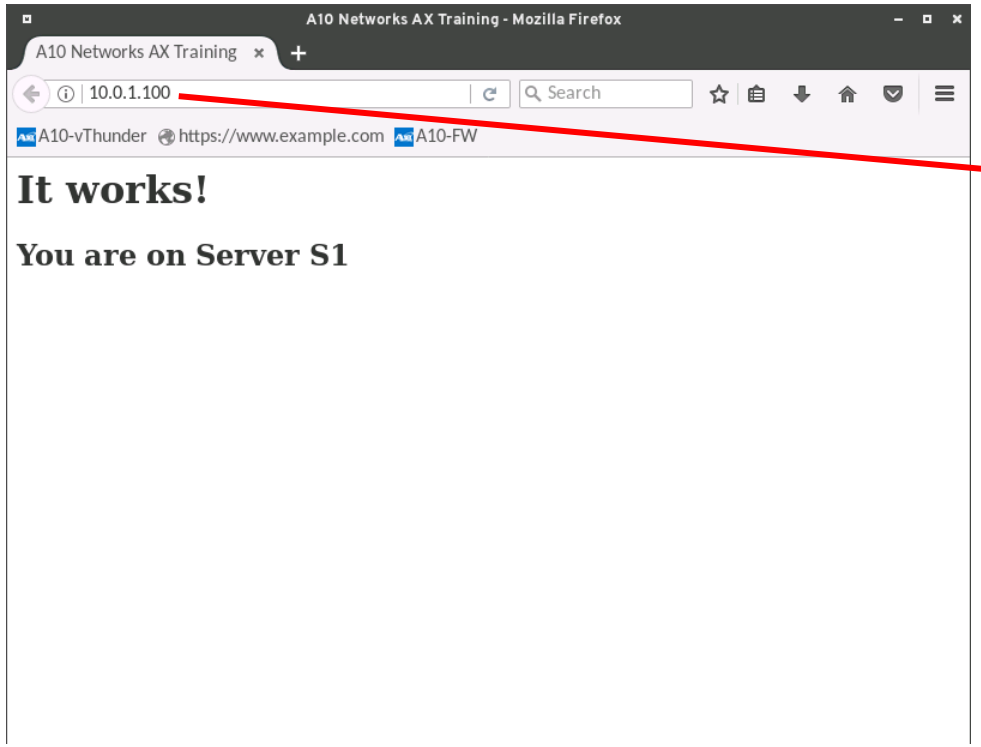
新規ServerSSLコネクション/秒

新規NATコネクション/秒

FWコネクション/秒

ラボ（２）基本サーバロードバランシング設定

5. 動作確認
   - ブラウザ(Firefox)から仮想IP（Virtual Server IP）へアクセス
   - Firefoxを起動して,アドレスバーに設定した仮想IPを入力し、“It works!”とコンテンツが表示できることを確認してください。



http://10.0.1.100/

作成したVirtual Serverの
IPアドレスを入力

ラボ（２）基本サーバロードバランシング設定

サンプルコンフィグ

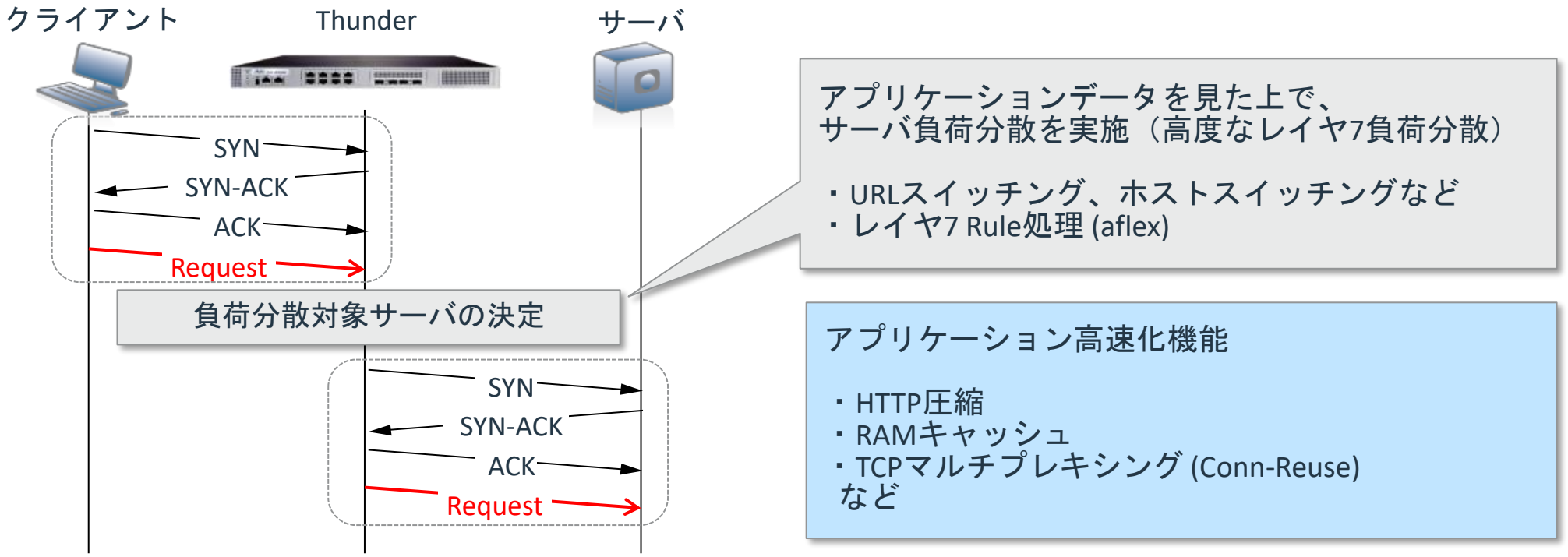
```
slb server s1 10.0.2.11
   port 80  tcp
!
slb server s2 10.0.2.12
   port 80  tcp
!
slb service-group sg-80 tcp
    method service-least-connection
    member s1 80
    member s2 80
!
slb virtual-server vip1 10.0.1.100
   port 80  tcp
     service-group sg-80
```

（４） アプリケーション負荷分散

WEB GUI による設定
※コマンドラインインターフェイス設定も可能

HTTP負荷分散のフルプロキシ・アーキテクチャ

「クライアント～Thunder」、「Thunder～サーバ」間それぞれでTCPコネクションを終端することにより、HTTPのプロトコルヘッダやデータの中身を見て負荷分散処理を行ったり、アプリケーションの高速化機能の利用が可能



アプリケーションデータを見た上で、
サーバ負荷分散を実施（高度なレイヤ7負荷分散）

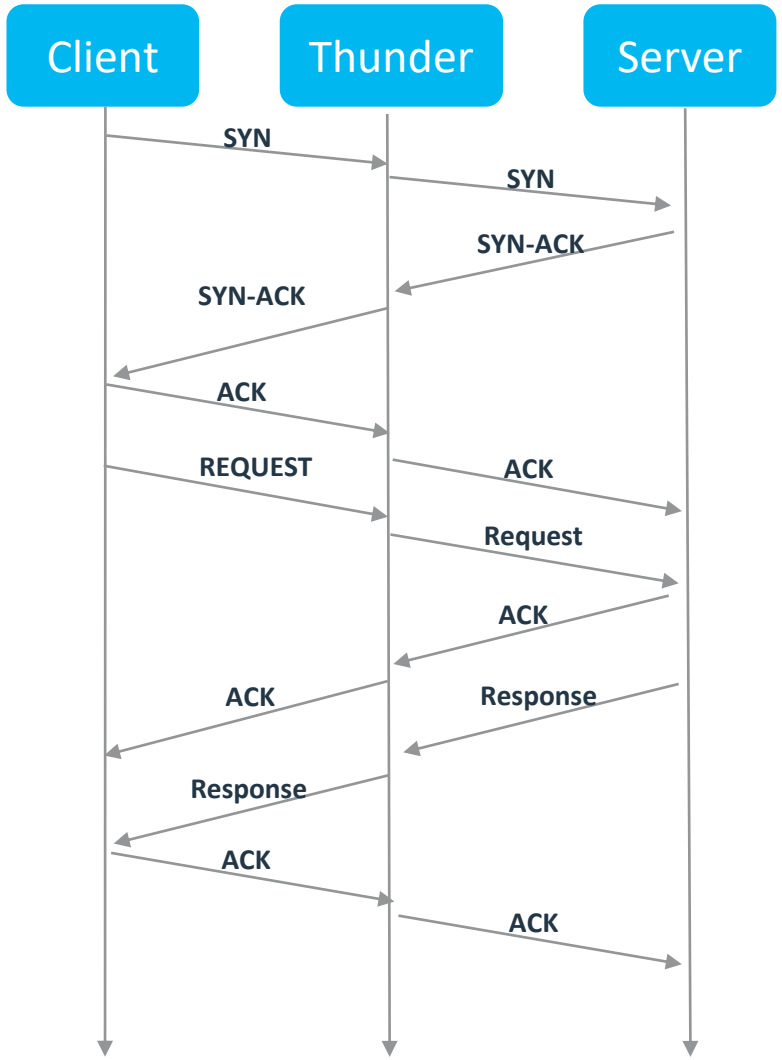
・URLスイッチング、ホストスイッチングなど
・レイヤ7 Rule処理 (aflex)

アプリケーション高速化機能

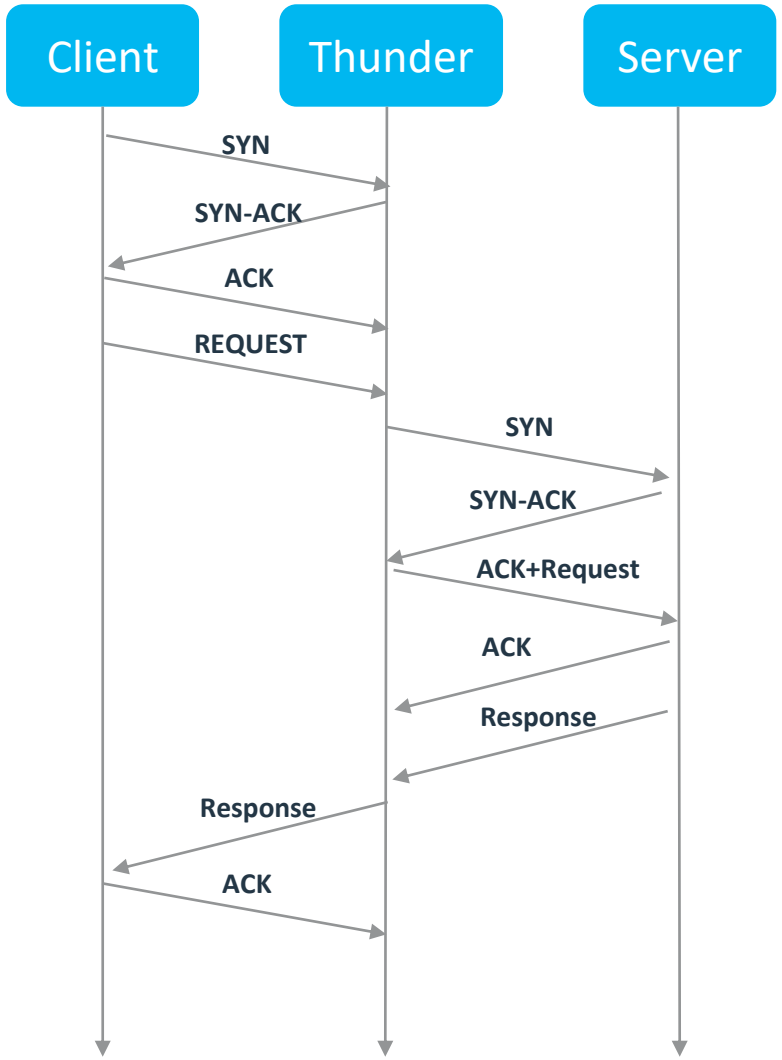
・HTTP圧縮
・RAMキャッシュ
・TCPマルチプレキシング (Conn-Reuse)
など

CPS Connection per second

L4 負荷分散

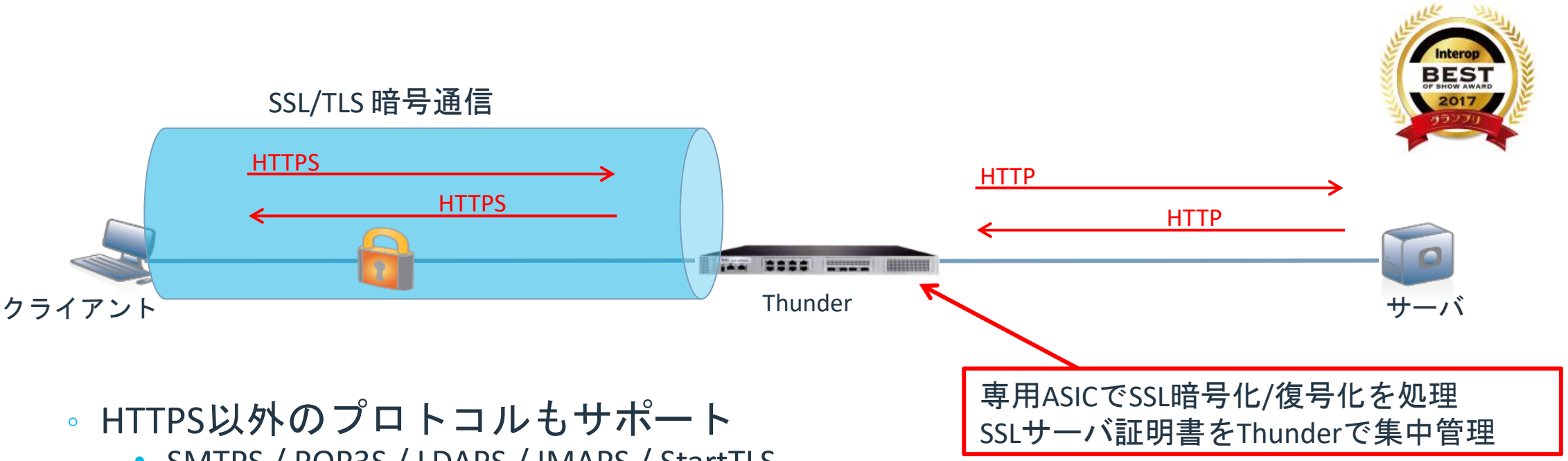


L7 負荷分散



HTTPS負荷分散のSSLアクセラレーション

クライアントとThunderの間でSSL暗号化 / 復号化を終端することにより
サーバ負荷を軽減



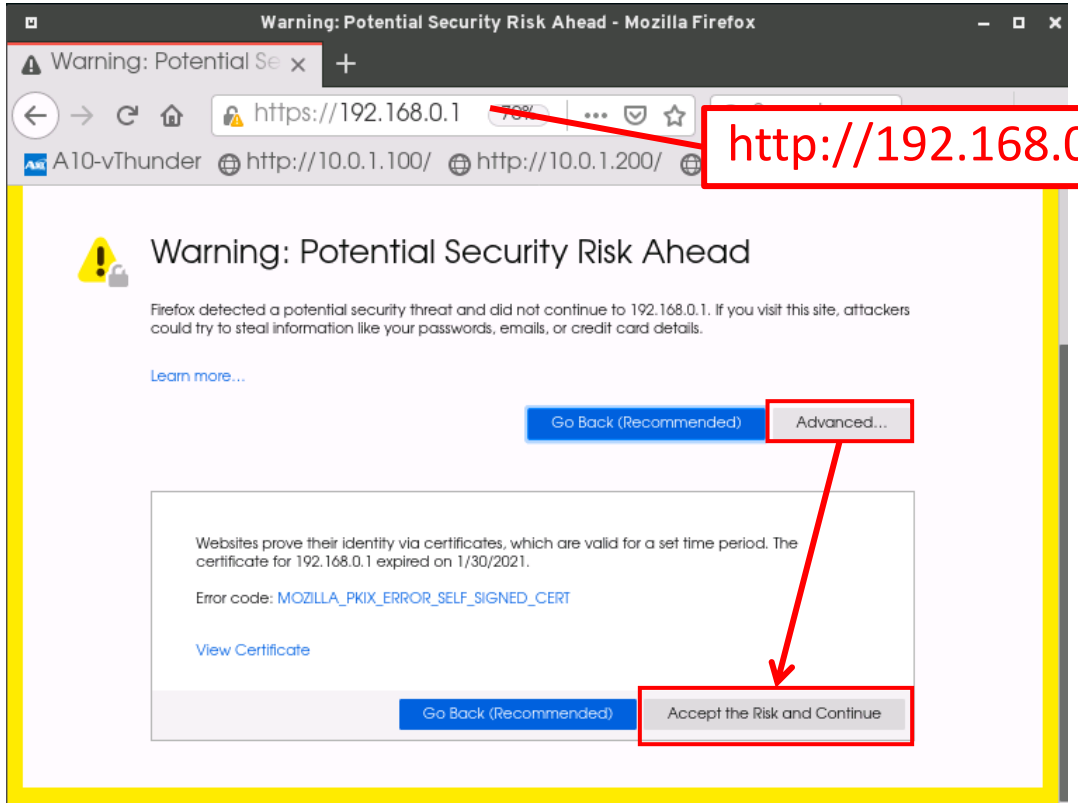
- HTTPS以外のプロトコルもサポート
  - SMTPS / POP3S / LDAPS / IMAPS / StartTLS

ラボ（３）環境設定

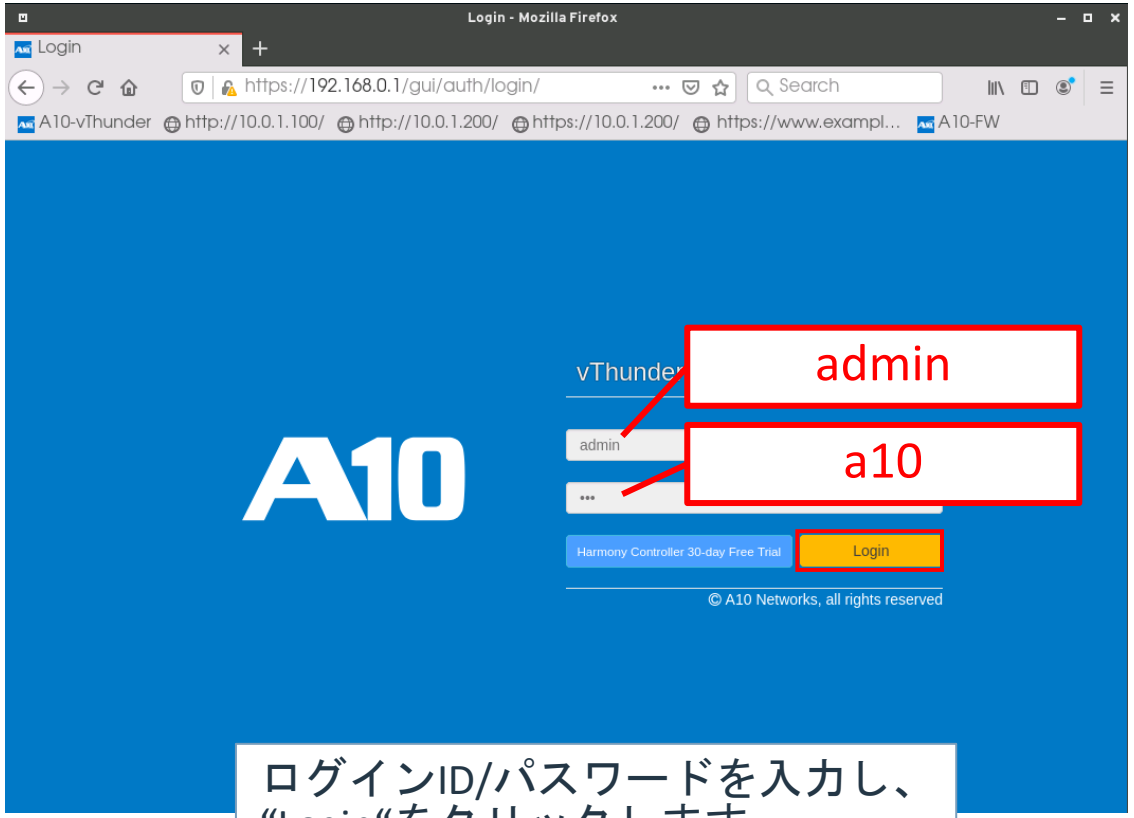
Server IP / Virtual Server IPアドレス割り当て

Thunder	Virtual-Server vip2
A10	10.0.1.200

ラボ（３）アプリケーション負荷分散設定



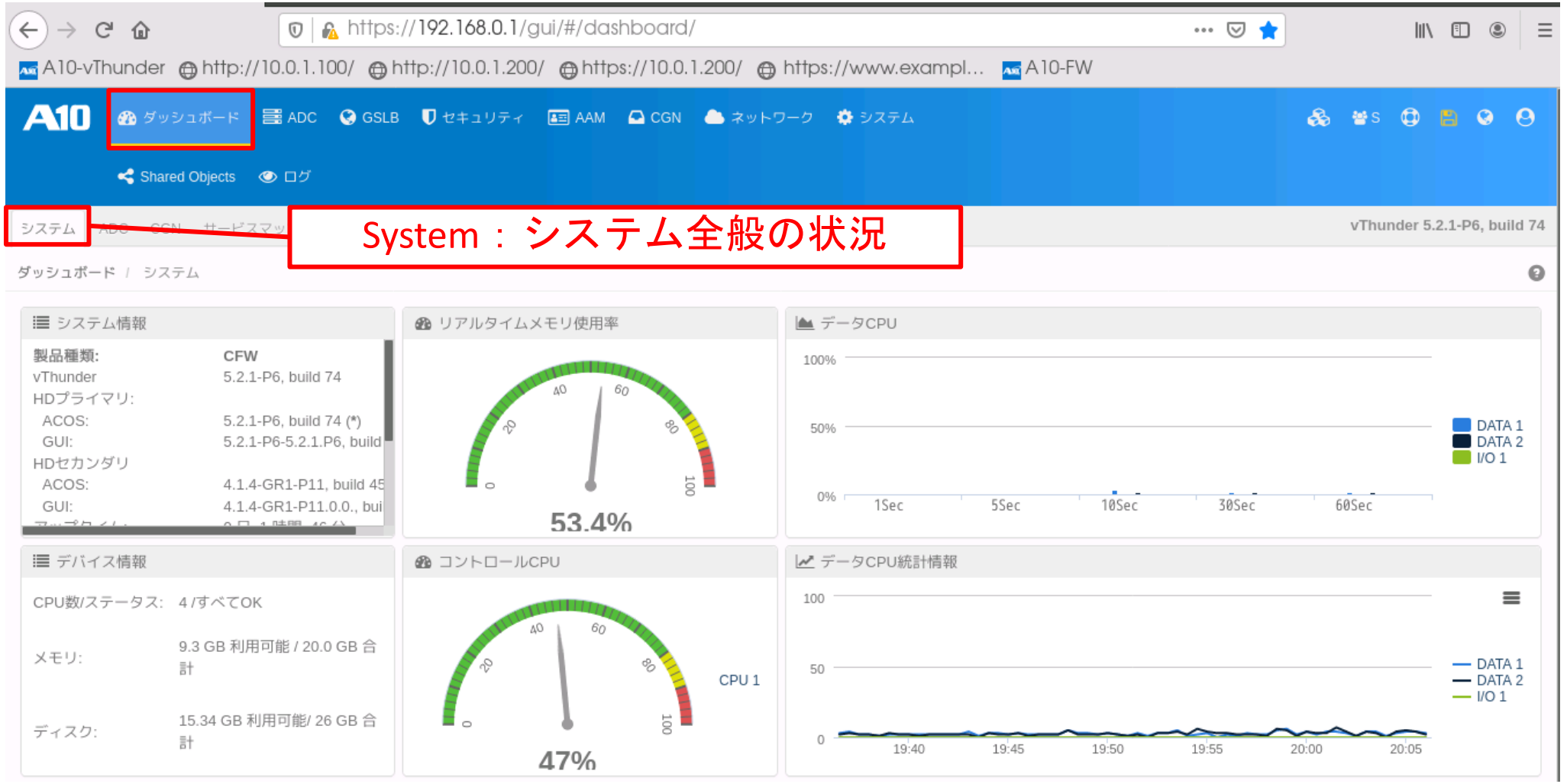
自己署名証明書のためセキュリティの警告が出ますが承認し、先に進めます。



ログインID/パスワードを入力し、“Login“をクリックします。

ラボ（３）アプリケーション負荷分散設定

WEB GUI TOP画面　ダッシュボード



ラボ（３）アプリケーション負荷分散設定

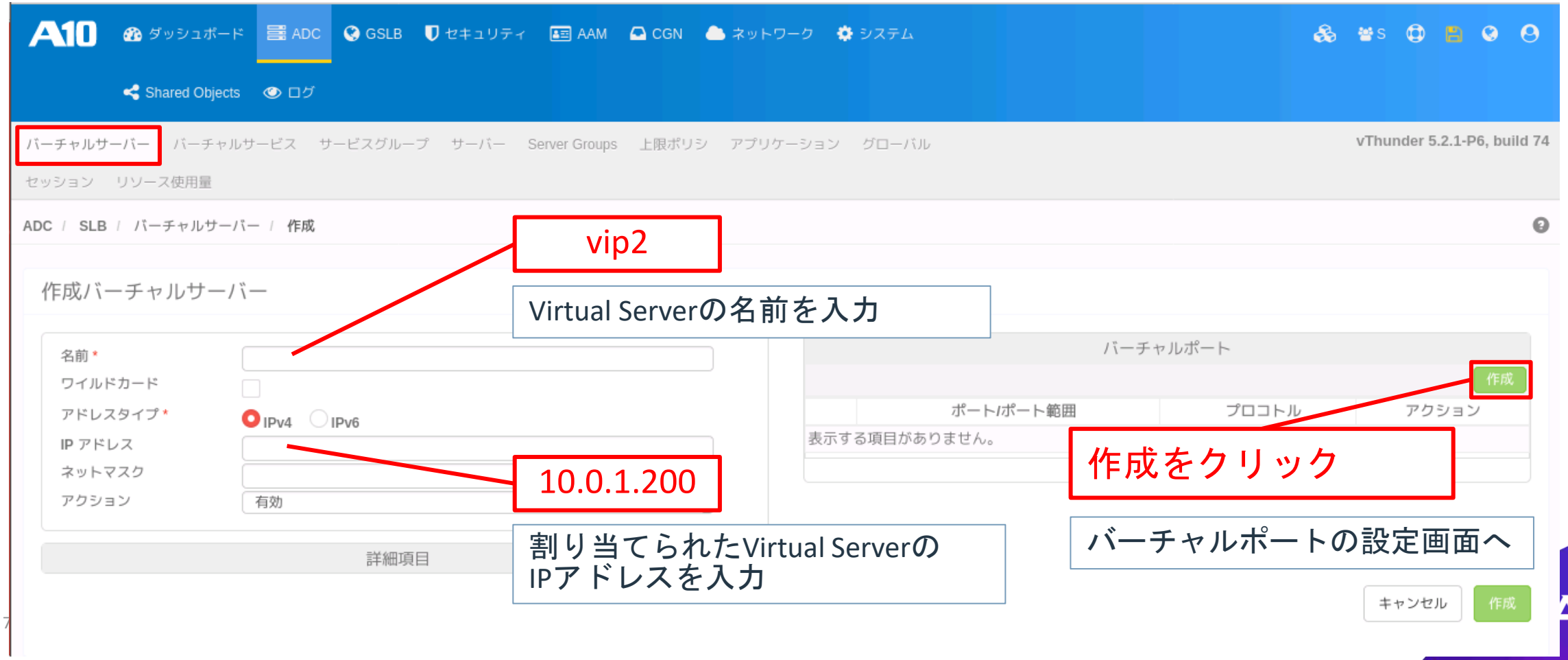
Virtual Serverの設定（HTTP）

ADC > SLB > Virtual Servers

ラボ（３）アプリケーション負荷分散設定

Virtual Serverの設定（HTTP）

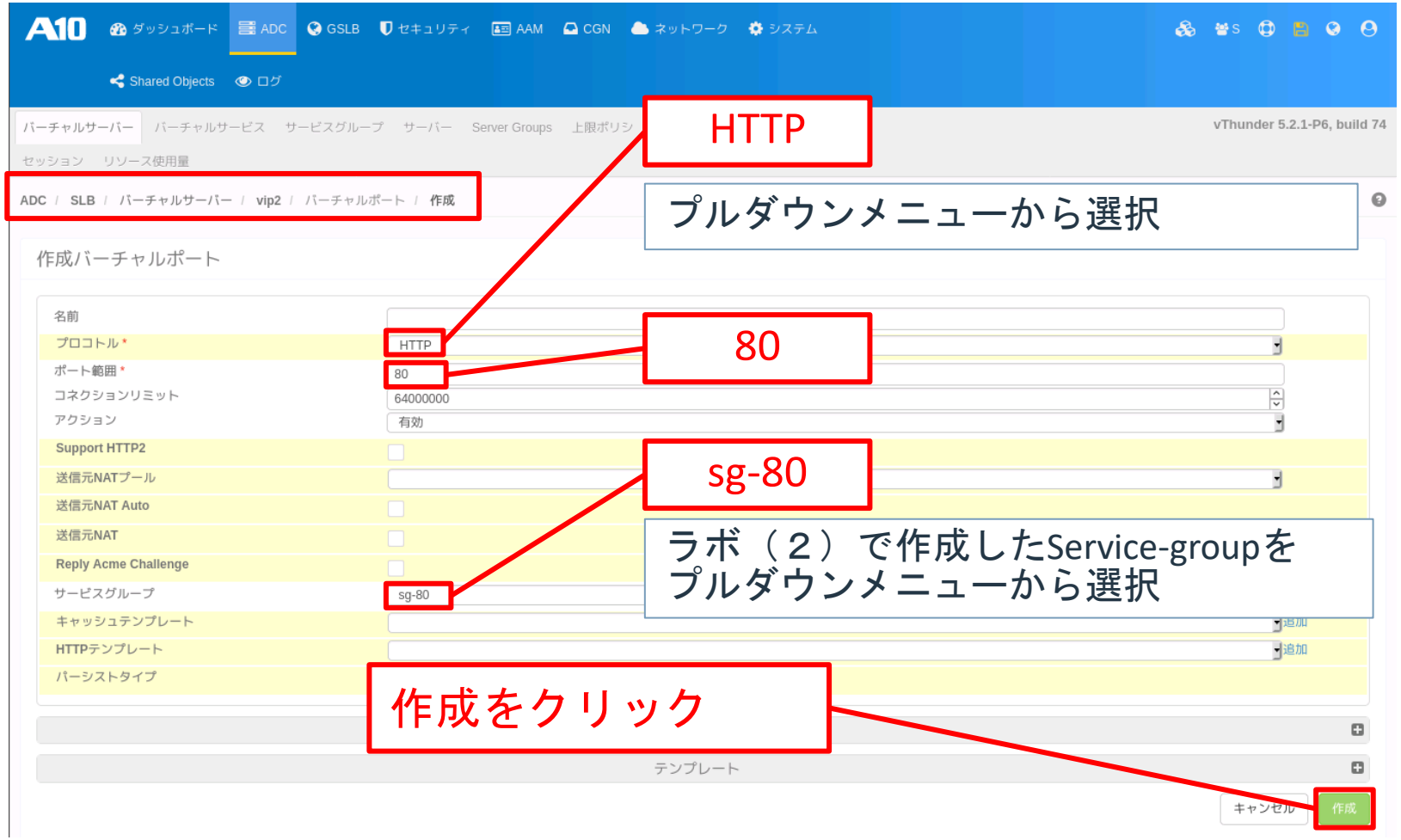
ADC > SLB > バーチャルサーバー> 作成



ラボ（３）アプリケーション負荷分散設定

Virtual Serverの設定（HTTP）

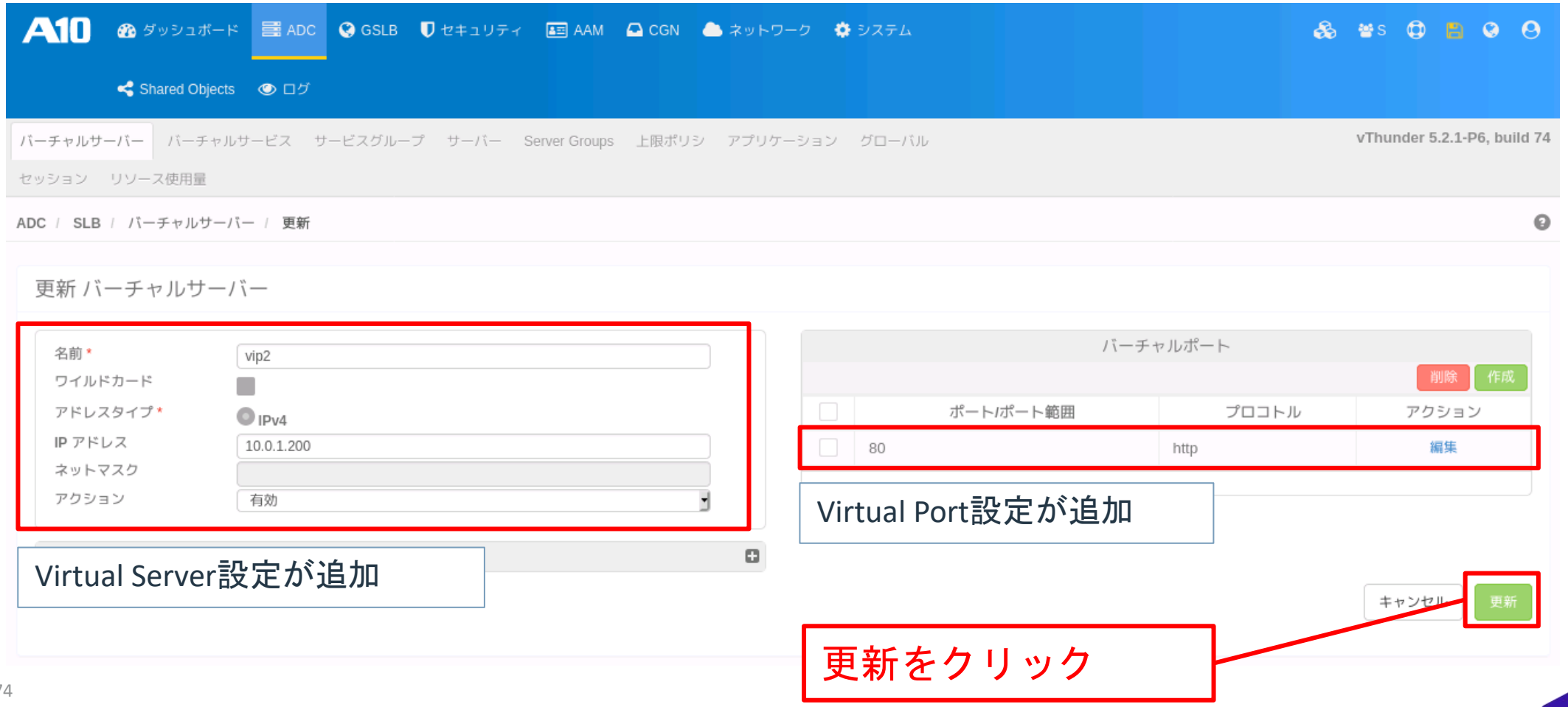
ADC > SLB > バーチャルサーバー > vip2 > バーチャルポート > 作成



ラボ（３）アプリケーション負荷分散設定

Virtual Serverの設定（HTTP）

ADC > SLB > バーチャルサーバー > 更新



ラボ（３）アプリケーション負荷分散設定

設定の確認（HTTP）

ADC > SLB > Virtual Servers

CLIで作成したvip1, GUIで設定したvip2 それぞれの ⊞ をクリックし展開、設定を確認

ラボ（３）アプリケーション負荷分散設定

動作の確認（HTTP）

ラボ（３）で作成した新しい仮想IPへアクセス

ラボ（３）アプリケーション負荷分散設定

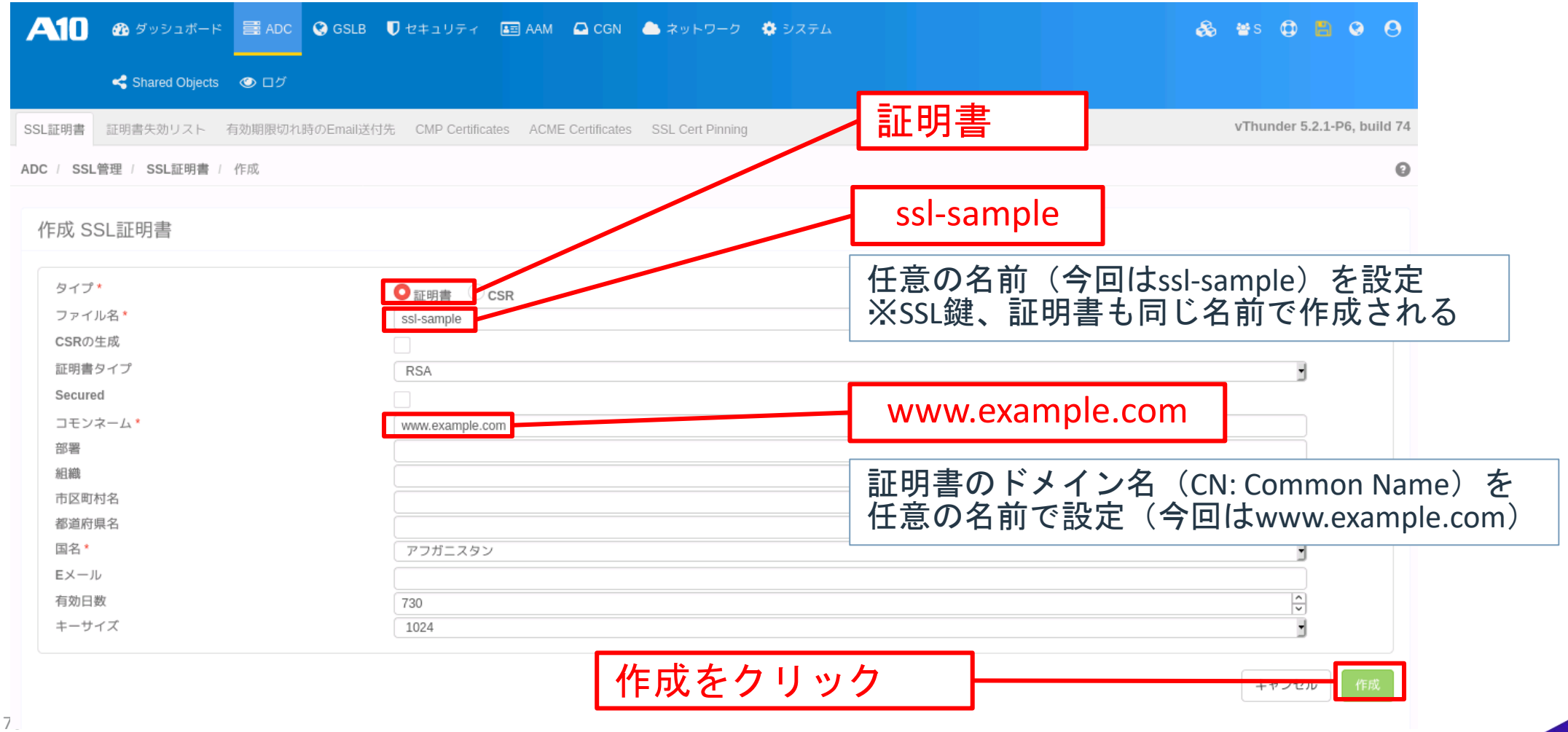
SSLオフロードの設定（SSL証明書、秘密鍵の作成・登録）

ADC > SSL 管理 > SSL 証明書

ラボ（３）アプリケーション負荷分散設定

SSLオフロードの設定（SSL証明書、秘密鍵の作成・登録）

ADC > SSL管理 > SSL証明書 > 作成



ラボ（３）アプリケーション負荷分散設定

SSLオフロードの設定（SSL証明書、秘密鍵の確認）

ADC > SSL 管理> SSL 証明書

certificate/keyペアが追加

ラボ（３）アプリケーション負荷分散設定

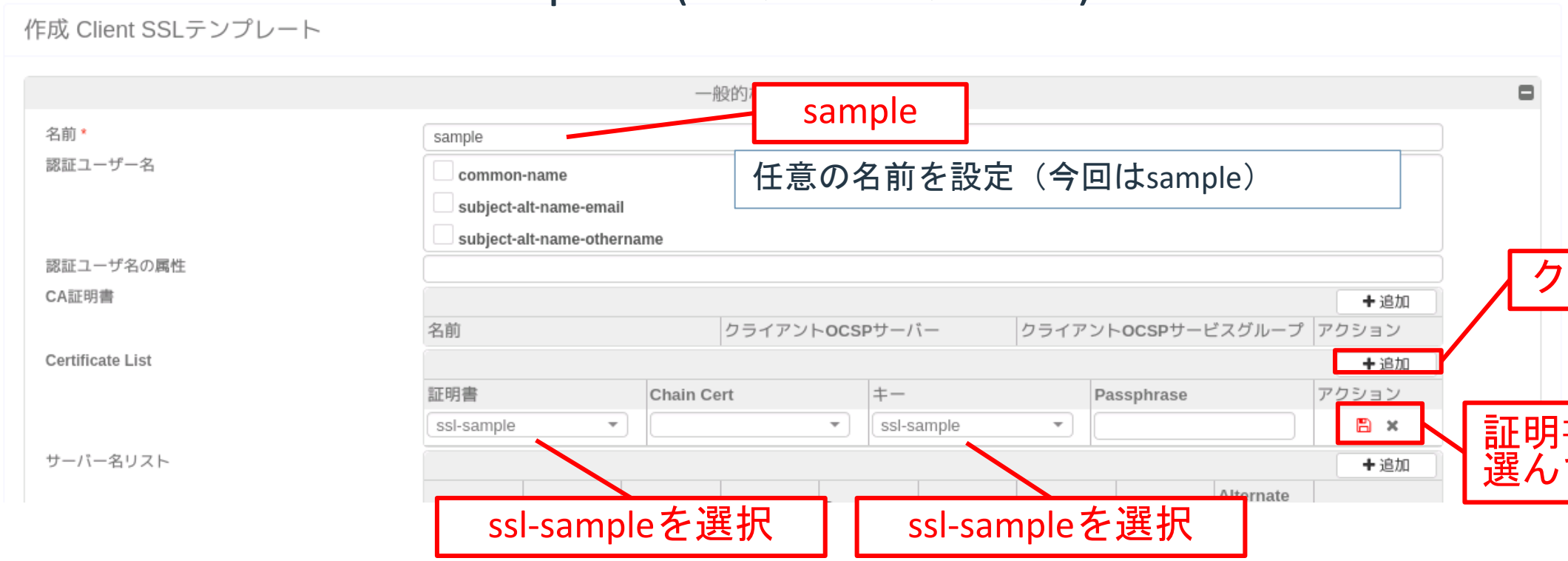
SSLテンプレートの設定

ADC > Templates > SSL

ラボ（３）アプリケーション負荷分散設定

SSLテンプレートの設定

Create Client SSL Template (ポップアップ窓)



ラボ（３）アプリケーション負荷分散設定

SSLテンプレートの確認

ADC > テンプレート > SSL

Client SSL Template設定が追加

ラボ（３）アプリケーション負荷分散設定

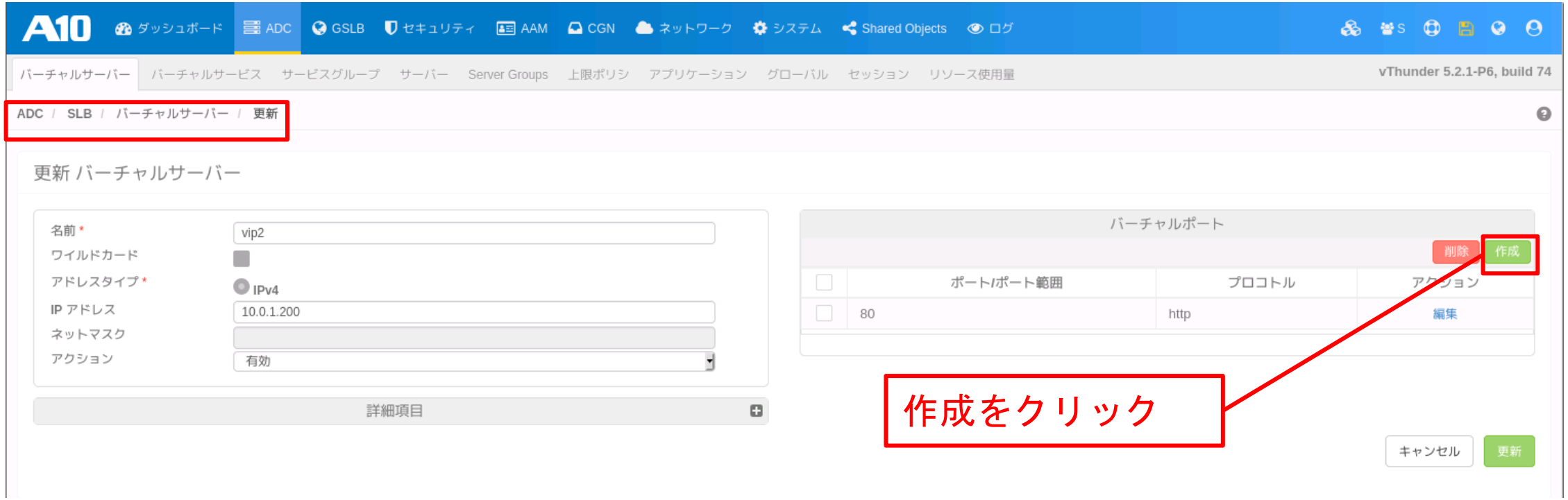
Virtual Serverの設定 （HTTPS）

ADC > SLB > Virtual Servers

ラボ（３）アプリケーション負荷分散設定

Virtual Serverの設定（HTTPS）

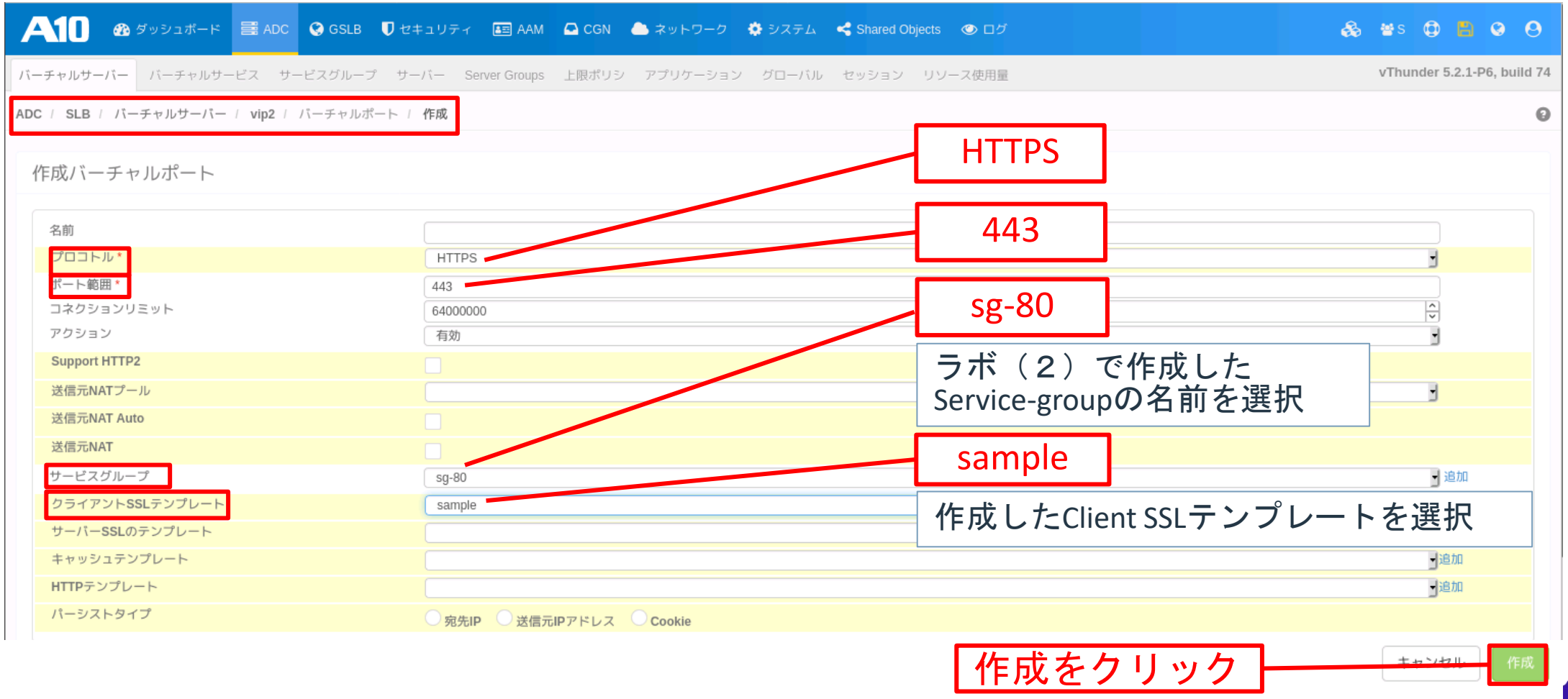
ADC > SLB > Virtual Servers > Update



ラボ（３）アプリケーション負荷分散設定

Virtual Serverの設定（HTTPS）

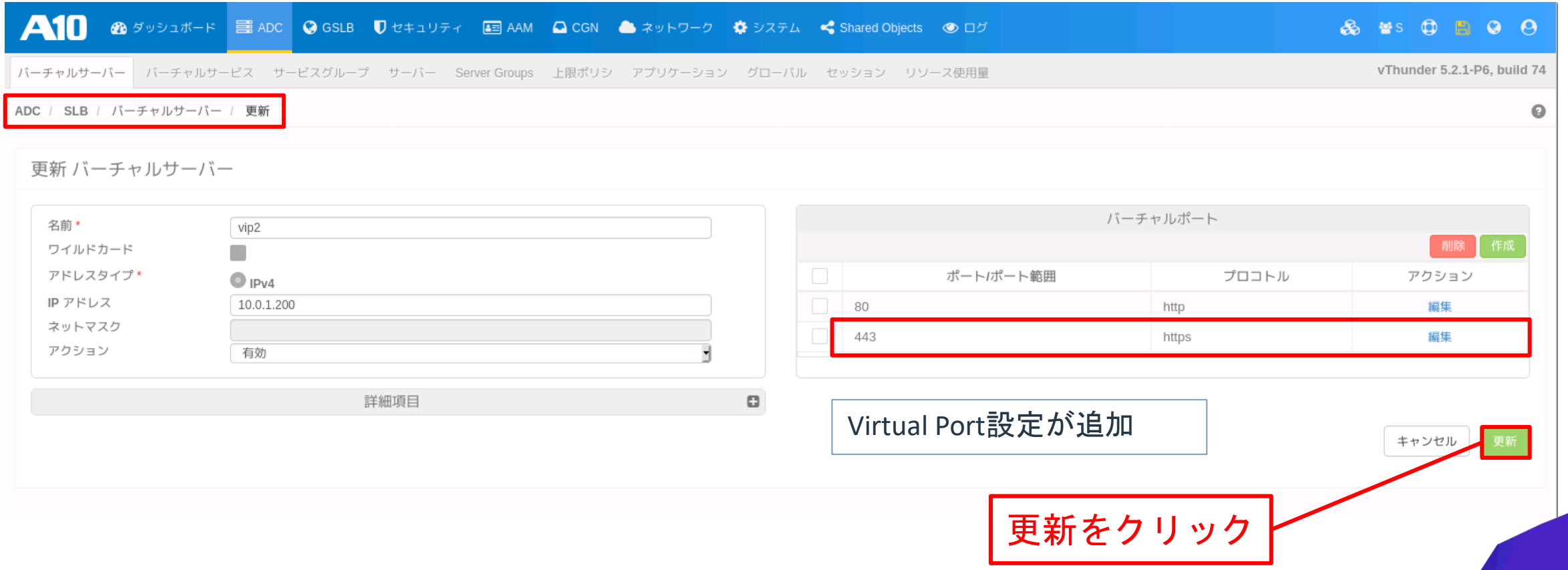
ADC > SLB > バーチャルサーバー > vip2 > バーチャルポート > 作成



ラボ（３）アプリケーション負荷分散設定

Virtual Serverの設定（HTTPS）

ADC > SLB > バーチャルサーバー > 更新



ラボ（３）アプリケーション負荷分散設定

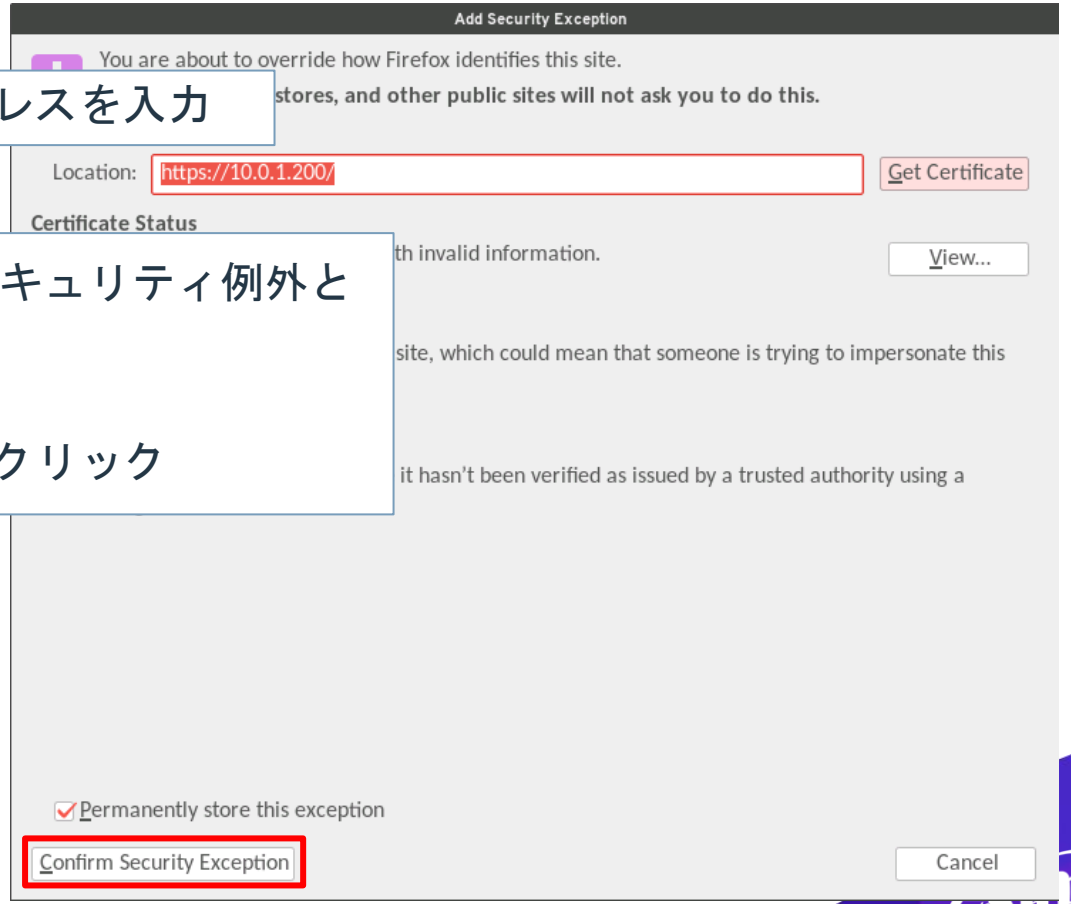
設定の確認（HTTPS）

ADC > SLB > Virtual Servers

ラボ（３）アプリケーション負荷分散設定

動作の確認（HTTPS）

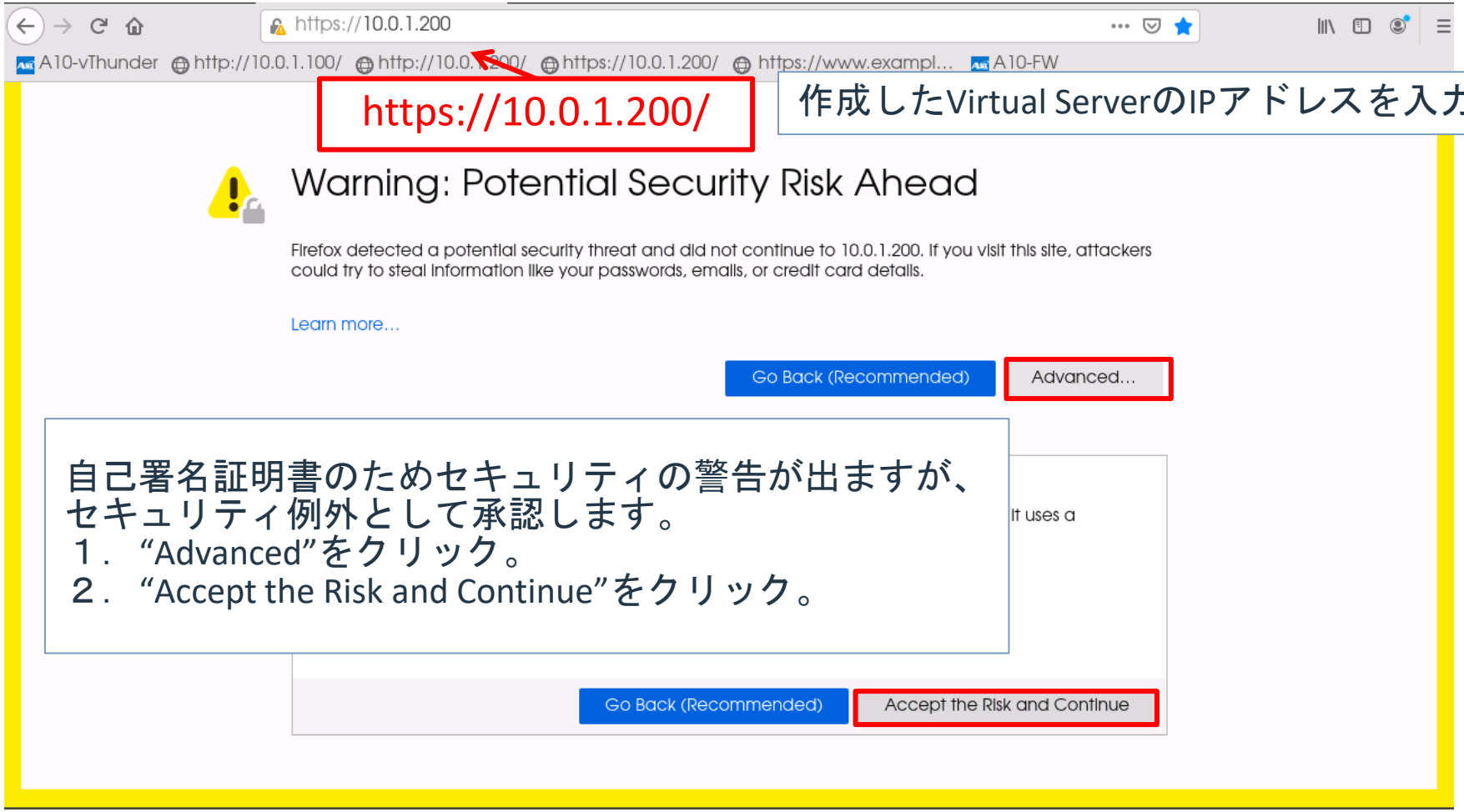
ラボ（３）で作成した新しい仮想IPへHTTPSでアクセス



ラボ（３）アプリケーション負荷分散設定

動作の確認（HTTPS）

ラボ（３）で作成した新しい仮想IPへHTTPSでアクセス



ラボ（３）アプリケーション負荷分散設定

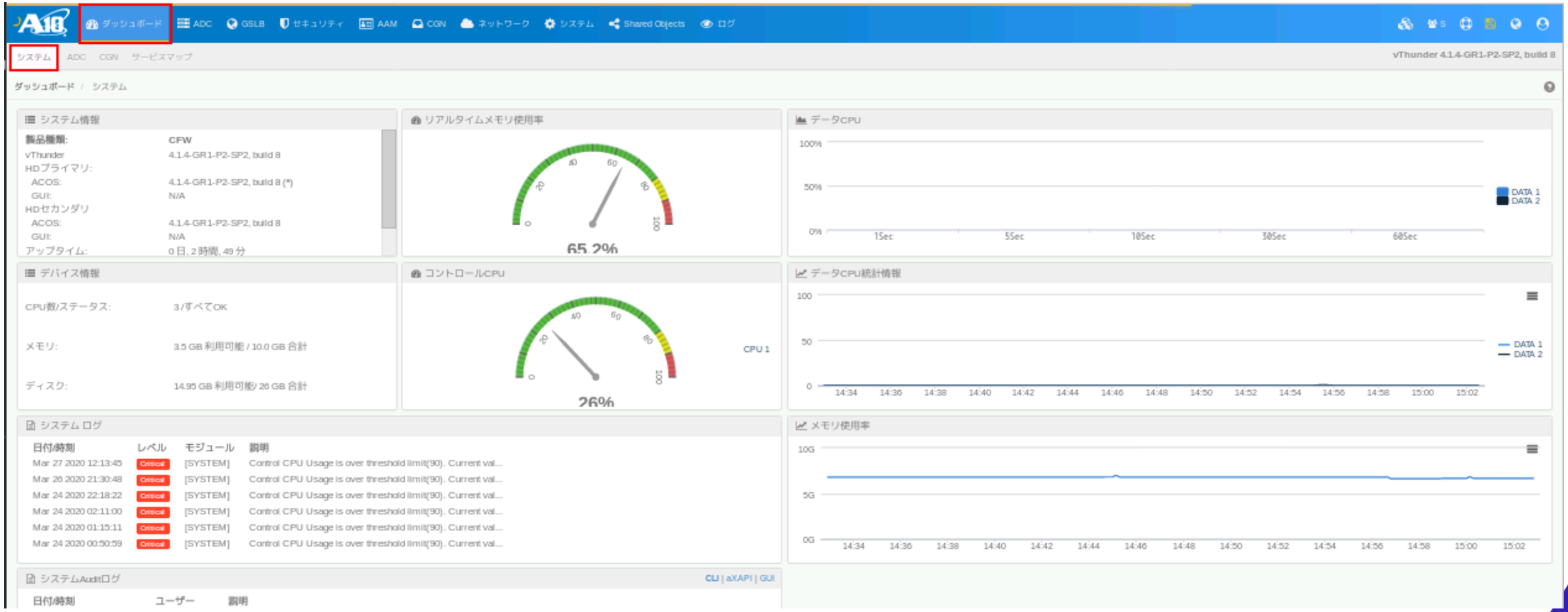
動作の確認（HTTPS）

以下のように“It works!”のページが表示されることを確認。

ラボ（3）GUI　ステータス確認

ステータスの確認（リソース）

ダッシュボード > システム



ラボ（３）アプリケーション負荷分散設定

ステータスの確認（パフォーマンス）

ADC > SLB > Virtual Servers

（5）ログのダウンロード

CLI/GUI による取得方法

show techsupport (CLI)

その時点のシステム、プロセスのステータス情報のスナップショットを出力

A10#show techsupport

============= Clock Info <Oct 10 2016 23:16:30.496850> =============

***08:16:30 JST Tue Oct 11 2016**

============= Version Info <Oct 10 2016 23:16:30.497444> =============

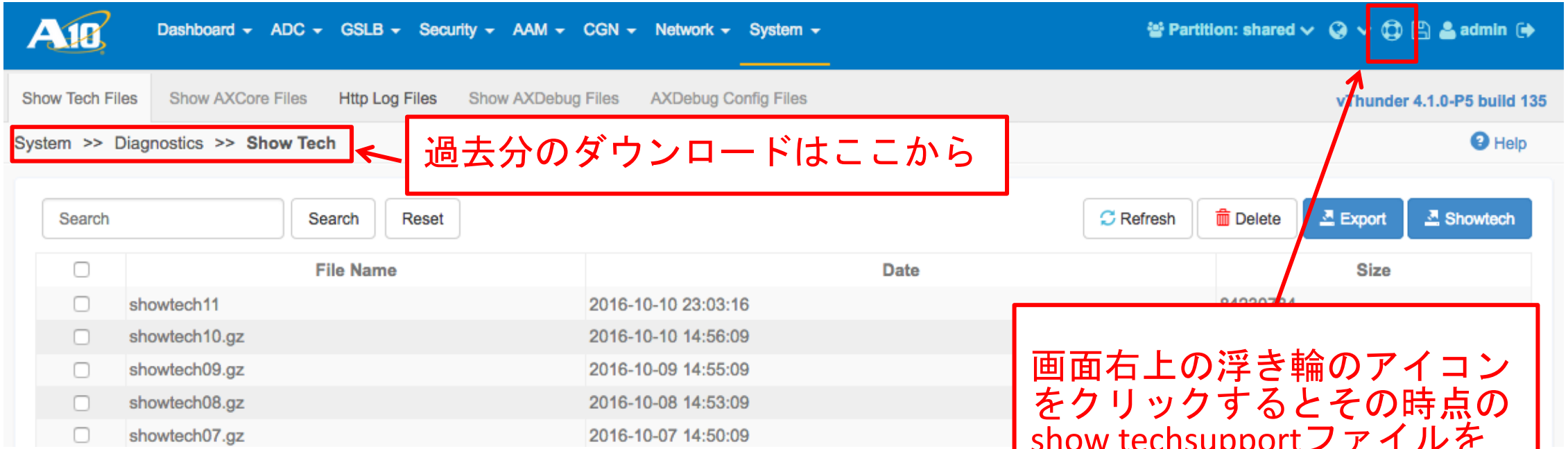
Thunder Series Unified Application Service Gateway vThunder

Copyright 2007-2016 by A10 Networks, Inc. All A10 Networks products are protected by one or more of the following US patents:.

:

:

show techsupport (GUI)



backup log

- Syslogに出力されないハードウェアログなどデバッグ用ログの保存
- 15分間隔でshow tech-supportの結果を最大1か月保存
- コアダンプファイル
- ログイン、変更履歴

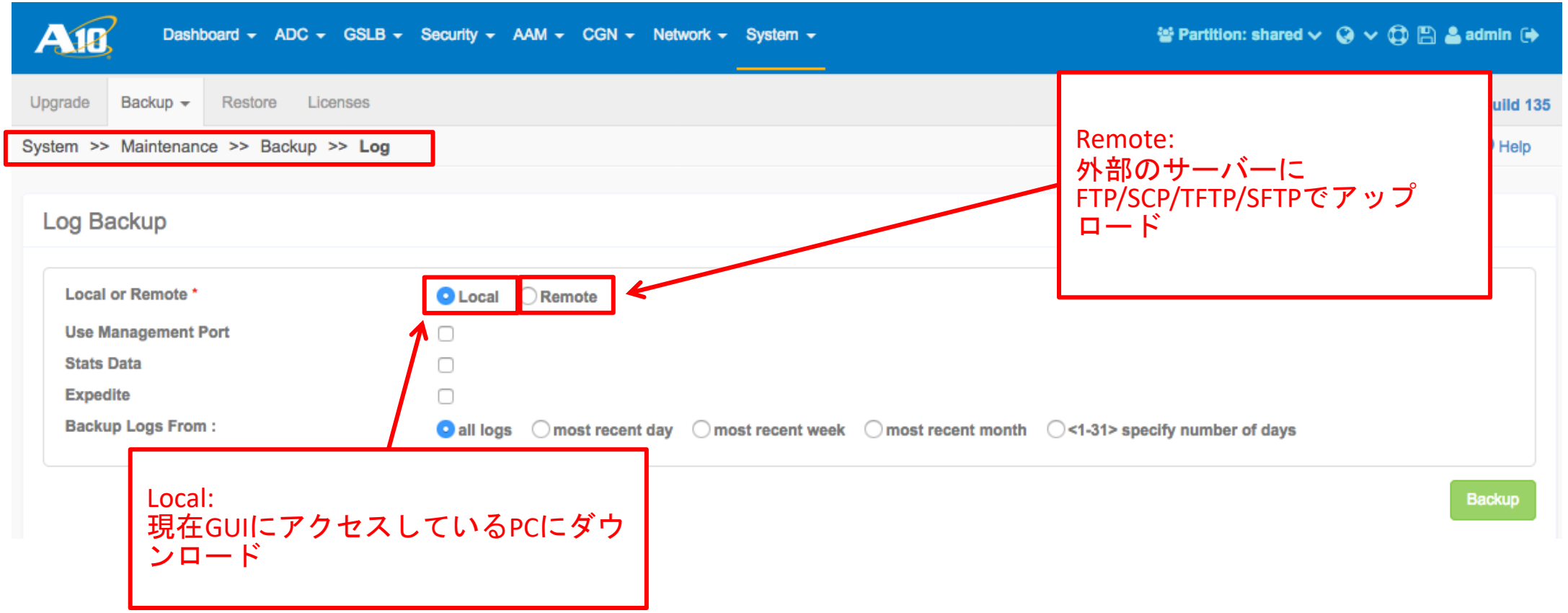
A10(config)#backup log use-mgmt-port scp://**student:a10**@192.168.0.100/home/student/Desktop

Backuplog files .....Log files backup succeeded

※上記ではアップロードするサーバーのID/パスワードはstudent/a10 となります。
※アップロード先サーバをご用意いただく必要があります。
※アップロードを行うプルトコルは tftp / ftp / scp / sftp が可能。

backup log (GUI)

System > Maintenance > Backup > Log



THANK YOU

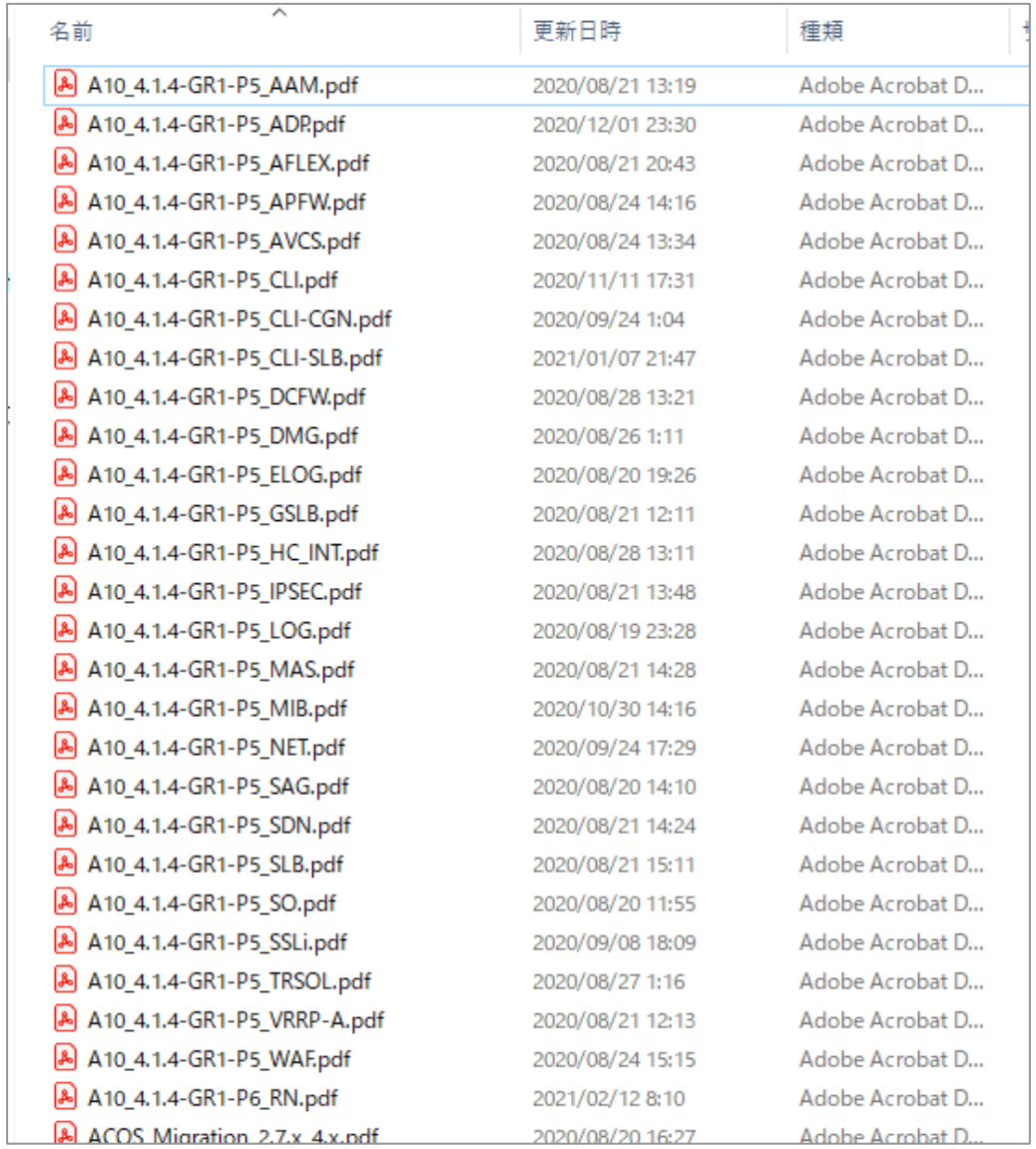
www.a10networks.co.jp

付録１：資料と基本操作

A10のマニュアル

A10_4.1.4-GR1-P8_PDF.zip

pdf



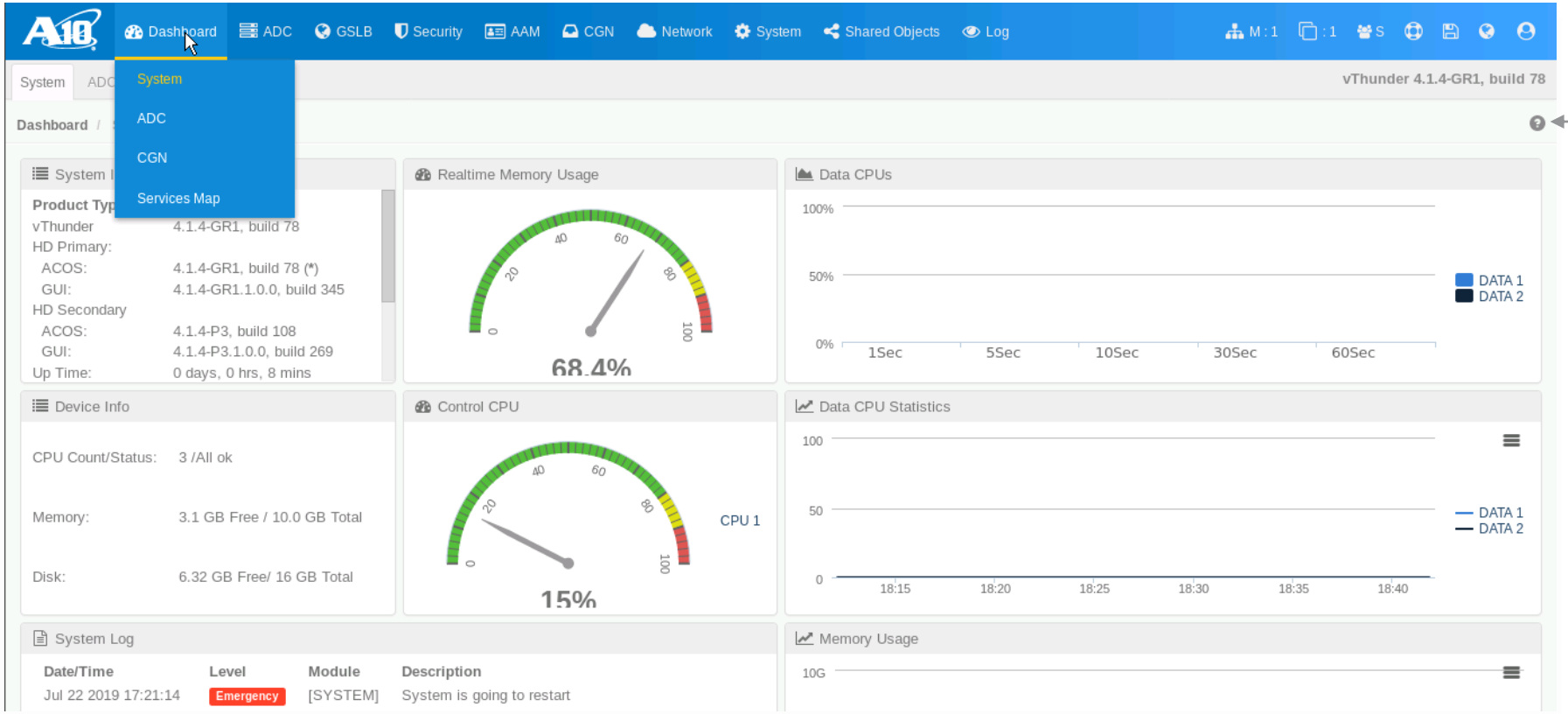
名前	更新日時	種類
A10_4.1.4-GR1-P5_AAM.pdf	2020/08/21 13:19	Adobe Acrobat D...
A10_4.1.4-GR1-P5_ADP.pdf	2020/12/01 23:30	Adobe Acrobat D...
A10_4.1.4-GR1-P5_AFLEX.pdf	2020/08/21 20:43	Adobe Acrobat D...
A10_4.1.4-GR1-P5_APFW.pdf	2020/08/24 14:16	Adobe Acrobat D...
A10_4.1.4-GR1-P5_AVCS.pdf	2020/08/24 13:34	Adobe Acrobat D...
A10_4.1.4-GR1-P5_CLI.pdf	2020/11/11 17:31	Adobe Acrobat D...
A10_4.1.4-GR1-P5_CLI-CGN.pdf	2020/09/24 1:04	Adobe Acrobat D...
A10_4.1.4-GR1-P5_CLI-SLB.pdf	2021/01/07 21:47	Adobe Acrobat D...
A10_4.1.4-GR1-P5_DCFW.pdf	2020/08/28 13:21	Adobe Acrobat D...
A10_4.1.4-GR1-P5_DMG.pdf	2020/08/26 1:11	Adobe Acrobat D...
A10_4.1.4-GR1-P5_ELOG.pdf	2020/08/20 19:26	Adobe Acrobat D...
A10_4.1.4-GR1-P5_GSLB.pdf	2020/08/21 12:11	Adobe Acrobat D...
A10_4.1.4-GR1-P5_HC_INT.pdf	2020/08/28 13:11	Adobe Acrobat D...
A10_4.1.4-GR1-P5_IPSEC.pdf	2020/08/21 13:48	Adobe Acrobat D...
A10_4.1.4-GR1-P5_LOG.pdf	2020/08/19 23:28	Adobe Acrobat D...
A10_4.1.4-GR1-P5_MAS.pdf	2020/08/21 14:28	Adobe Acrobat D...
A10_4.1.4-GR1-P5_MIB.pdf	2020/10/30 14:16	Adobe Acrobat D...
A10_4.1.4-GR1-P5_NET.pdf	2020/09/24 17:29	Adobe Acrobat D...
A10_4.1.4-GR1-P5_SAG.pdf	2020/08/20 14:10	Adobe Acrobat D...
A10_4.1.4-GR1-P5_SDN.pdf	2020/08/21 14:24	Adobe Acrobat D...
A10_4.1.4-GR1-P5_SLB.pdf	2020/08/21 15:11	Adobe Acrobat D...
A10_4.1.4-GR1-P5_SO.pdf	2020/08/20 11:55	Adobe Acrobat D...
A10_4.1.4-GR1-P5_SSLi.pdf	2020/09/08 18:09	Adobe Acrobat D...
A10_4.1.4-GR1-P5_TRSOL.pdf	2020/08/27 1:16	Adobe Acrobat D...
A10_4.1.4-GR1-P5_VRRP-A.pdf	2020/08/21 12:13	Adobe Acrobat D...
A10_4.1.4-GR1-P5_WAF.pdf	2020/08/24 15:15	Adobe Acrobat D...
A10_4.1.4-GR1-P6_RN.pdf	2021/02/12 8:10	Adobe Acrobat D...
ACOS_Migration_2.7.x_4.x.pdf	2020/08/20 16:27	Adobe Acrobat D...

A10のマニュアル

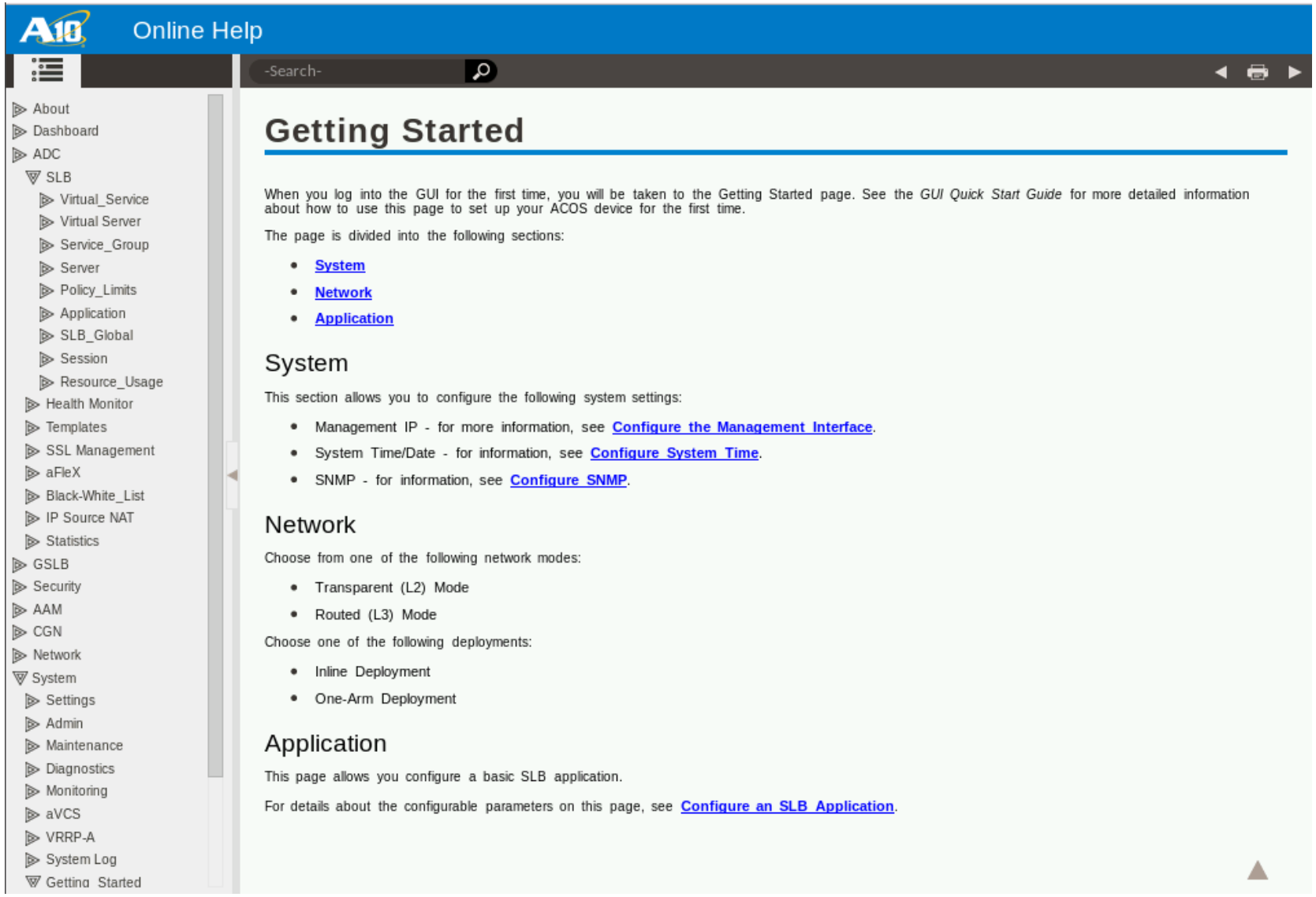
AAM: Application Access Management
ADP: Application Delivery Partitions
AFLEX: aFleX Scripting
APFW: Application Firewall
AVCS: ACOS Virtual Chassis Systems
CLI: Command Line
CLI-CGN: Command for CGN
CLI-SLB: Command for ADC
DCFW: Firewall
DMG: DDoS mitigation (for ADC)
ELOG: Event Logging
GSLB: Global Server Load Balancinge
HC_INT: HarmonyController
IPSEC: IPsec VPN

LOG: Logging for IPv6 Migration
MAS: Management Access and Security Guide
MIB: SNMP MIB
NET: Network
RN: Release Notes
SAG: System and Administration
SDN: Overlay Networks
SLB: Application Delivery Controller
SO: Scaleout
SSLi: SSL Insight
TRSOL: IPv4-to-IPv6 Transition
VRRP-A: VRRP-A High Availability
WAF: Web Application Firewall

GUI:設定するオブジェクトをまとめた形で配置



GUI：ヘルプドキュメント表示



CLI：コンフィグのインデント

[コンフィグ例]

```
slb virtual-server vip2 10.0.1.200
   port 80 http
      service-group sg-80
```

```
A10#configure
A10(config)#slb virtual-server vip2
A10(config-slb vserver)#port 80 http
A10(config-slb vserver-vport)#service-group sg-80
A10(config-slb vserver-vport)#exit
A10(config-slb vserver)#exit
A10(config)#exit
A10#
```

Ctrl-CはconfigモードのexitのキーボードショートカットCtrl-Zはconfigモードのendのキーボードショートカット

```
A10#configure
A10(config)#slb virtual-server vip2
A10(config-slb vserver)#port 80 http
A10(config-slb vserver-vport)#service-group sg-80
A10(config-slb vserver-vport)#end
A10#
```

CLI：ヘルプ

リストオプション

- ACOS> **show health monitor ?**
- WORD<length:1-31> Name
  all-partitions All partition configurations
  partition Per-partition configurations
  | Output modifiers

オプションの曖昧さ回避

- ACOS> **show ic?**
- icmp Display ICMP statistics
  icmpv6 Display ICMPv6 statistics

コマンドの完了

- ACOS> **show rad*<tab>***
  ACOS> show radius-server

コマンドの連続実行

- ACOS> **repeat 1 show cpu** //1秒に一回実行
  ACOS> **repeat 5 show interfaces statistics** //5秒に一回実行

Running-configの確認
CLI フィルタリング（section & include）

ACOSは、sectionおよびincludeに出力をパイピングすることにより出力内容をフィルタリングすることが可能である。

sectionはコンフィグ要素を取得

```
ACOS#show run | sec slb
slb server S1 10.0.2.18
   port 80  tcp
slb service-group HTTP tcp
   member s1 80
```

includeは指定文字列を含む行を取得

```
ACOS#show run | inc slb
slb server S1 10.0.2.18
slb service-group HTTP tcp
```

Running-configの確認方法（OR検索）

「|」記号をORとしてincまたはsecで使用するには、

「¥」(バックスラッシュ)でエスケープする（前後にスペースなし）。

```
ACOS#show run | inc tacacs¥|radius
tacacs-server host 1.0.0.100 secret (encrypted_secret) port 49 timeout 12
radius-server host 1.0.0.100 secret (encrypted_secret)
```

CLI：管理系

```
ACOS# show version ;ACOSのバージョン、格納されているACOS、Uptime等を確認する。
ACOS# show running-config ;running-configはコンフィグをメモリに保存され、設定は即時反映される。
ACOS# show startup-config ;startup-configはディスクに保存される。
ACOS# write memory  ;現在のコンフィグ設定をディスクに保存する。
ACOS# write memory <コンフィグ名>  ;設定を新規コンフィグ名でディスクに保存する。
ACOS# show startup-config all  ;保存済みコンフィグのリストを表示する。
ACOS(config)#link startup-config <コンフィグ名> <primary/secondary> ;リロード・リブート時のコンフィグを指定する。
ASOS(config)#bootimage hd <pri/sec> ;次回起動時に起動するOSを設定する。
ACOS# show bootimage ;次回起動時に起動するOSを表示する。
ACOS# reload ;リロード(コンフィグの読み込み)
ACOS# reboot ;再起動(コンフィグの読み込み、OSの読み込み)
ACOS# shutdown ;A10のシャットダウン
ACOS# backup system use-mgmt-port scp://ユーザ名@サーバーIP/パス/  ;システムのバックアップ
ACOS# restore use-mgmt-port scp://ユーザ名@サーバーIP/パス/xxx.tar.gz ;システムのリストア
ACOS# system-reset ;A10を出荷状態に戻す。注意：コンフィグの削除、管理IPが172.31.31.31に戻される。
```

基本情報 sh version

使用しているACOSのVersion情報を確認

```
vThunder#sh ver
Thunder Series Unified Application Service Gateway vThunder
  Copyright 2007-2019 by A10 Networks, Inc.  All A10 Networks products are
  protected by one or more of the following US patents:
  10243791, RE47296,  10230770, 10187423, 10187377, 10178165, 10158627
  10129122, 10116634, 10110429, 10091237, 10069946, 10063591, 10044582
  10038693, 10027761, 10021174, 10020979, 10002141
  9992229, 9992107, 9986061, 9979801, 9979665, 9961136, 9961135, 9961130
  9960967, 9954899, 9954868, 9942162, 9942152, 9912555, 9912538, 9906591
  9906422, 9900343, 9900252, 9860271, 9848013, 9843599, 9843521, 9843484
  9838472, 9838425, 9838423, 9825943, 9806943, 9787581, 9756071, 9742879
  9722918, 9712493, 9705800, 9661026, 9621575, 9609052, 9602442, 9596286
  9596134, 9584318, 9544364, 9537886, 9531846, 9497201, 9477563, 9398011
  9386088, 9356910, 9350744, 9344456, 9344421, 9338225, 9294503, 9294467
  9270774, 9270705, 9258332, 9253152, 9231915, 9219751, 9215275, 9154584
  9154577, 9124550, 9122853, 9118620, 9118618, 9106561, 9094364, 9060003
  9032502, 8977749, 8943577, 8918857, 8914871, 8904512, 8897154, 8868765
  8849938, 8826372, 8813180, 8782751, 8782221, RE44701, 8595819, 8595791
  8595383, 8584199, 8464333, 8423676, 8387128, 8332925, 8312507, 8291487
  8266235, 8151322, 8079077, 7979585, 7804956, 7716378, 7665138, 7675854
  7647635, 7627672, 7596695, 7577833, 7552126, 7392241, 7236491, 7139267
  6748084, 6658114, 6535516, 6363075, 6324286, 8392563, 8103770, 7831712
  7606912, 7346695, 7287084, 6970933, 6473802, 6374300

          64-bit Advanced Core OS (ACOS) version 4.1.4-GR1-P6, build 90 (Feb-09-2021,07:37)
          Booted from Hard Disk primary image
          Number of control CPUs is set to 1
          Serial Number: vThunder1000015819
          aFleX version: 2.0.0
          GUI primary image (default) version 4_1_4-GR1-P6-4_1_4-gr1-p6-29
          GUI secondary image version
          aXAPI version: 3.0
          Cylance version: N/A
          Hard Disk primary image (default) version 4.1.4-GR1-P6, build 90
          Hard Disk secondary image version 5.2.1-p1, build 56
          Last configuration saved at Apr-20-2021, 17:13
          Virtualization type: KVM
          System Polling Mode: On
          Hardware: 4 CPUs(Stepping 1), Single 26G drive, Free storage is 11G
          Total System Memory 20517 Mbytes, Free Memory 9504 Mbytes
          Hardware Manufacturing Code: N/A
          Current time is Sep-27-2021, 12:15
          The system has been up 0 day, 0 hour, 25 minutes
vThunder#
```

基本情報 sh version

```
64-bit Advanced Core OS (ACOS) version 4.1.4-GR1-P6, build 90 (Feb-09-2021,07:37)
Booted from Hard Disk primary image
Number of control CPUs is set to 1
Serial Number: vThunder1000015819
aFleX version: 2.0.0
GUI primary image (default) version 4_1_4-GR1-P6-4_1_4-gr1-p6-29
GUI secondary image version
aXAPI version: 3.0
Hard Disk primary image (default) version 4.1.4-GR1-P6, build 90
Hard Disk secondary image version 5.2.1-p1, build 56
Last configuration saved at Apr-20-2021, 17:13
Virtualization type: KVM
System Polling Mode: On
Hardware: 4 CPUs(Stepping 1), Single 26G drive, Free storage is 11G
Total System Memory 20517 Mbytes, Free Memory 9504 Mbytes
Hardware Manufacturing Code: N/A
The system has been up 0 day, 0 hour, 25 minutes
vThunder#
```

1．使用中のバージョン番号
2．格納されているACOSのバージョン番号
3．ACOSが起動している時間

ACOSのファイルについて

■ACOSファイル一覧

○NonFTAモデル
　　ファイル名： ACOS_non_FTA_(バージョン名).upg

○FTAモデル
　　ファイル名： ACOS_FTA_(バージョン名).upg

○FTA v2モデル
　　ファイル名：ACOS_FTA_V2_(バージョン名).upg

○仮想版ACOSイメージ
　　Baremetal(ISO)　　: ACOS_Baremetal_(バージョン名).iso
　　vThunder(ISO)　　: ACOS_vThunder_(バージョン名).iso
　　vThunder(ESXi)　　: ACOS_vThunder_(バージョン名).ova.gz
　　vThunder(KVM)　　: vThunder_(バージョン名).qcow2.gz
　　vThunder(HyperV) : vThunder_(バージョン名).vhd.gz

ACOSファイルについて

■NonFTAモデル：
TH3040S,TH3030S,TH1040(S),TH1030S,TH940,TH930,TH840(S),AX3530,**vThunder**

ファイル名　：ACOS_non_FTA_(バージョン名).upg

■FTA v2モデル：
TH5330(S),TH3430(S),TH3230(S)

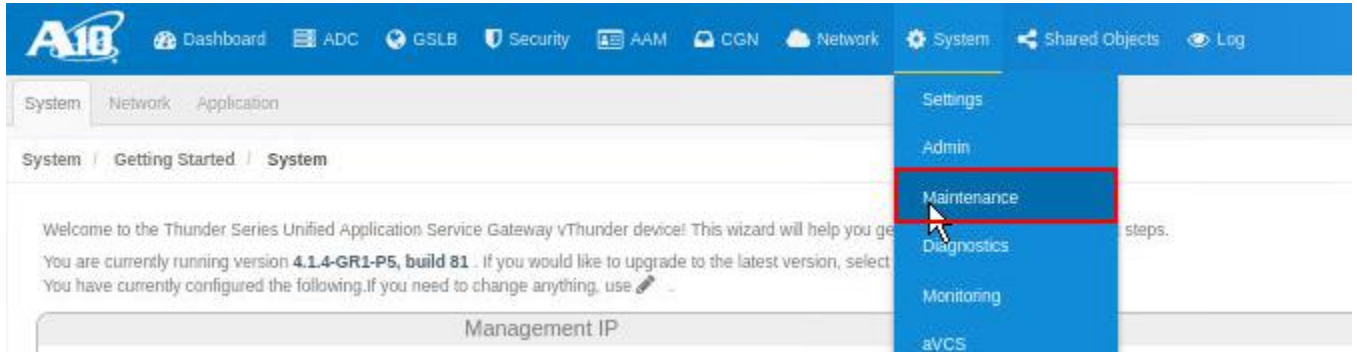
ファイル名　：ACOS_FTA_**V2**_(バージョン名).upg

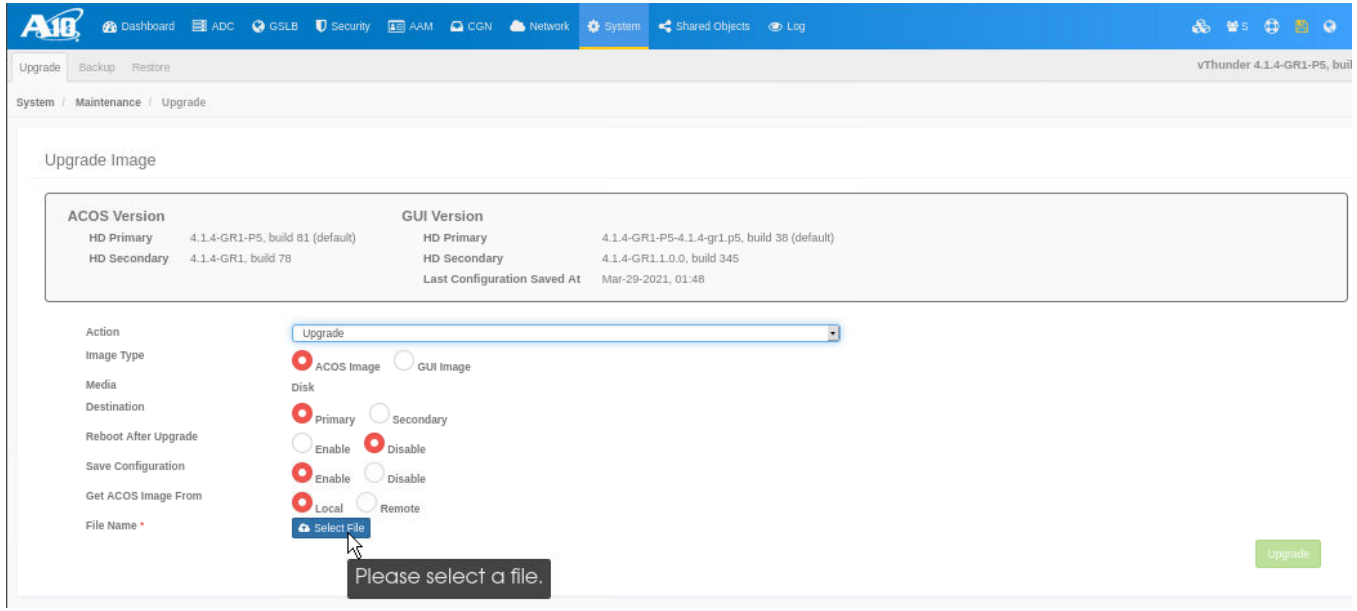
■FTA モデル　：
TH14045,TH7445(S),TH7440(S)-11, TH7440(S),TH6635(S),TH6630(S),TH6440(S),TH6435(S),TH6430(S),TH5845(S),
TH5840(S),TH5630(S),TH5440(S),TH5435(S),TH5430(S)-11,TH4440(S),TH4435(S),TH4430(S),AX5630

ファイル名　：ACOS_FTA_(バージョン名).upg

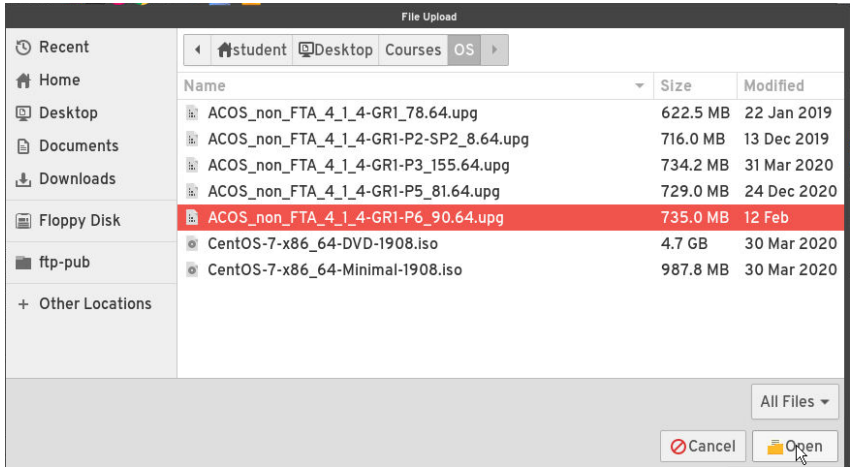
ACOSバージョン変更

- GUI(systems→Maintenance→Upgrade)



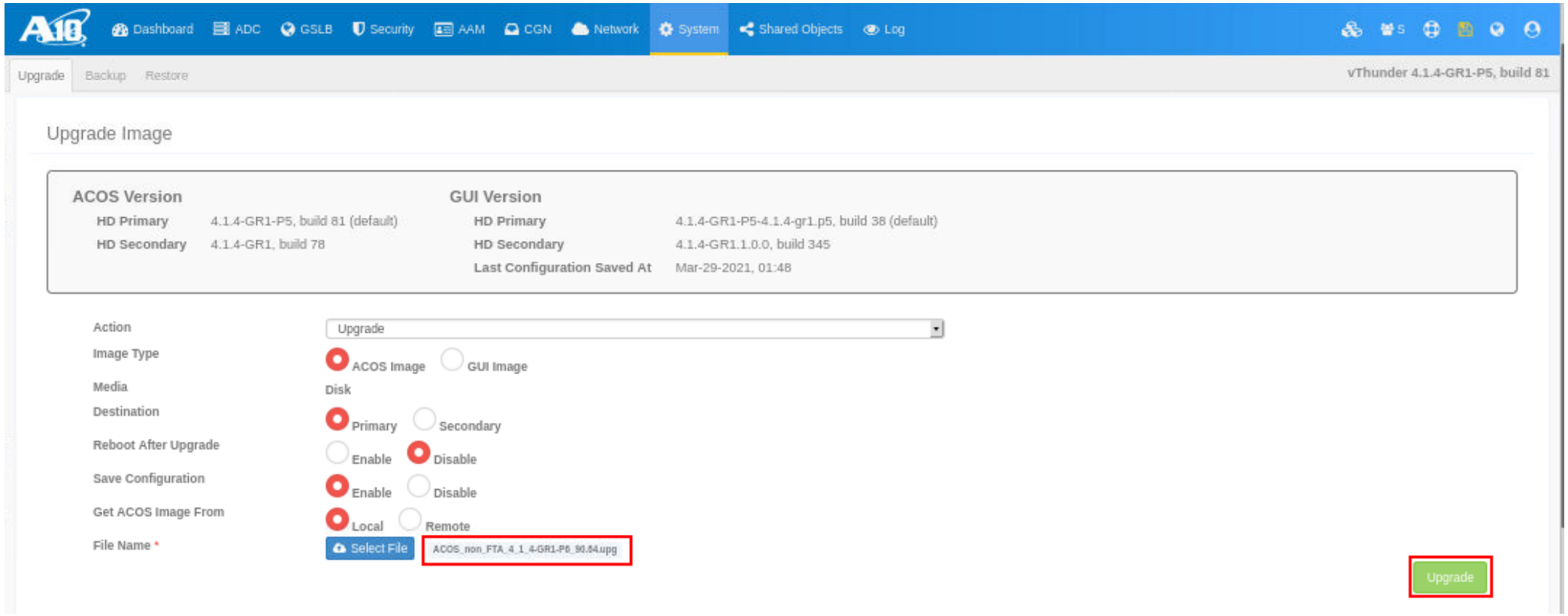


- 変更するACOSファイルを選択する



ACOSバージョン変更

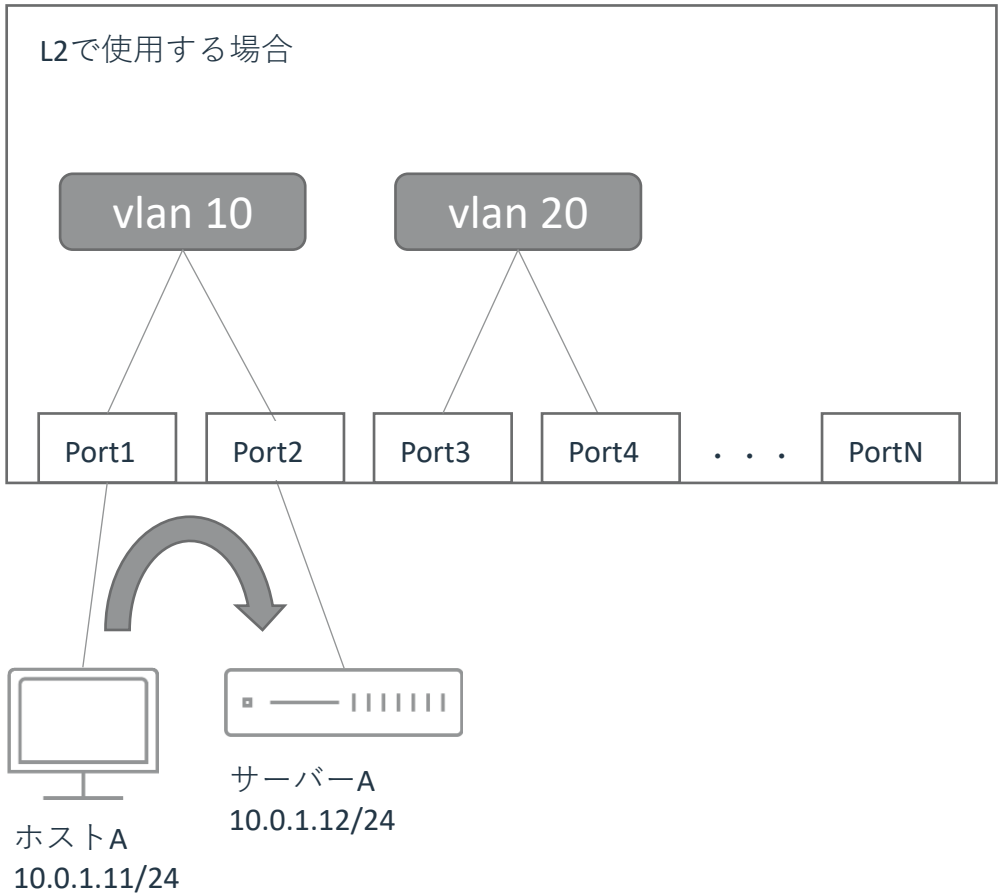
- ファイルを選択して“Upgarde”をクリック

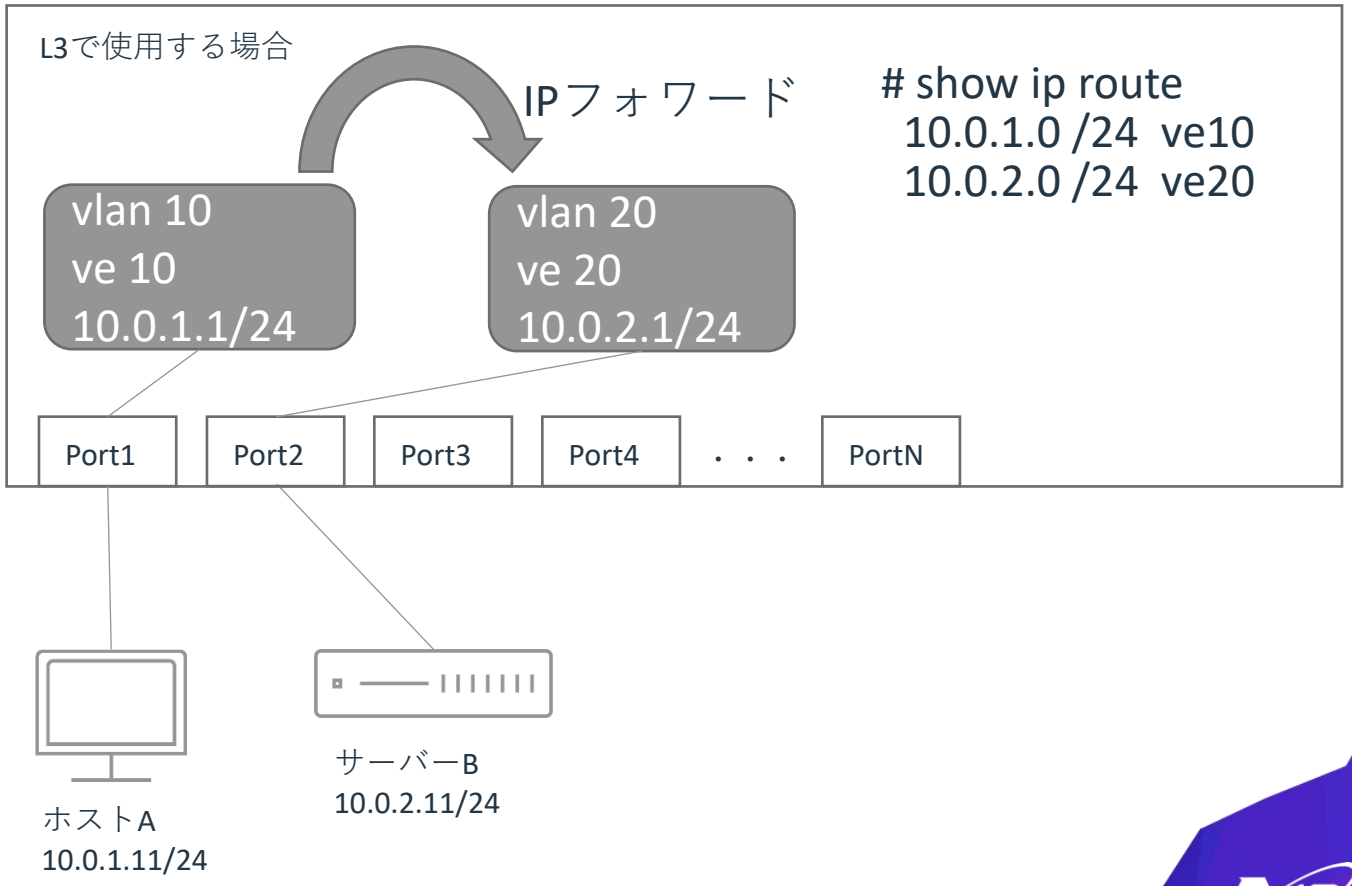


“Reboot after upgrade” を上記では無効にしているため、
ACOSファイルのインポートだけが行われる。
新規バージョンで動かすにはOSの格納場所(primary/second)を指定して再起動する。
CLIでのバージョン変更はマニュアルを参照してください。

[補足] vlanについて

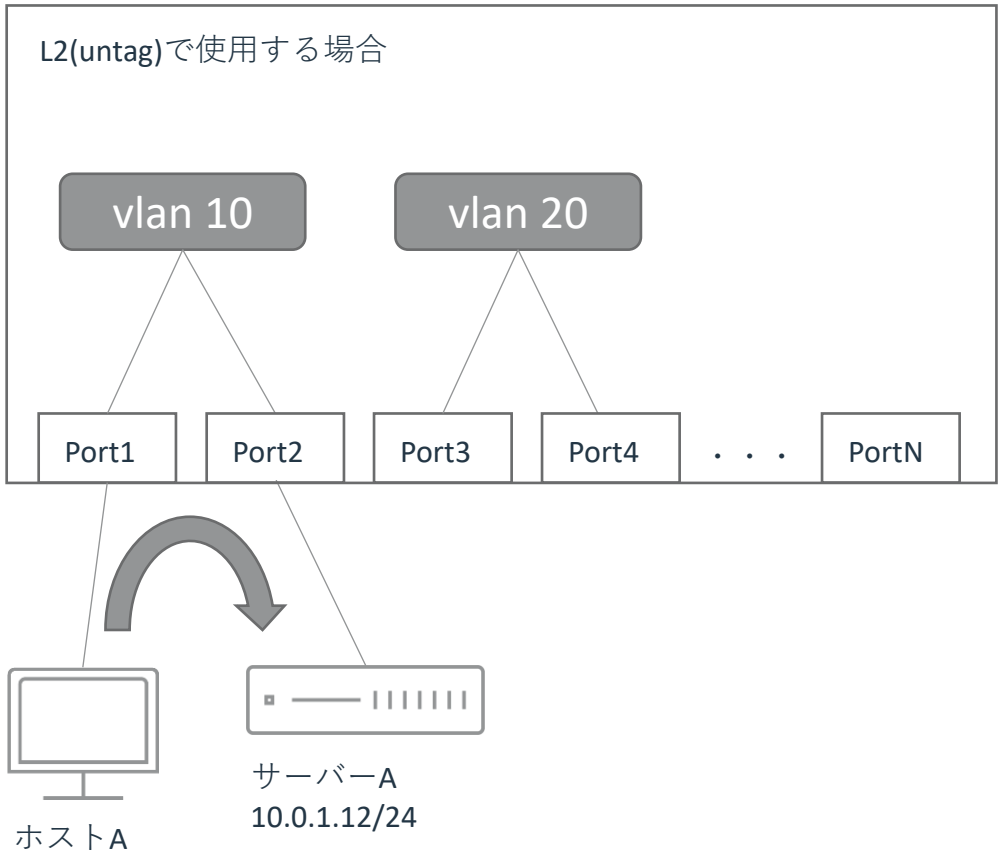
A10にはL2/L3スイッチの機能が搭載されており、
VLANは通常、L2/3では以下のように使用します。





[補足]vlanインターフェイス(L2で使用する場合)

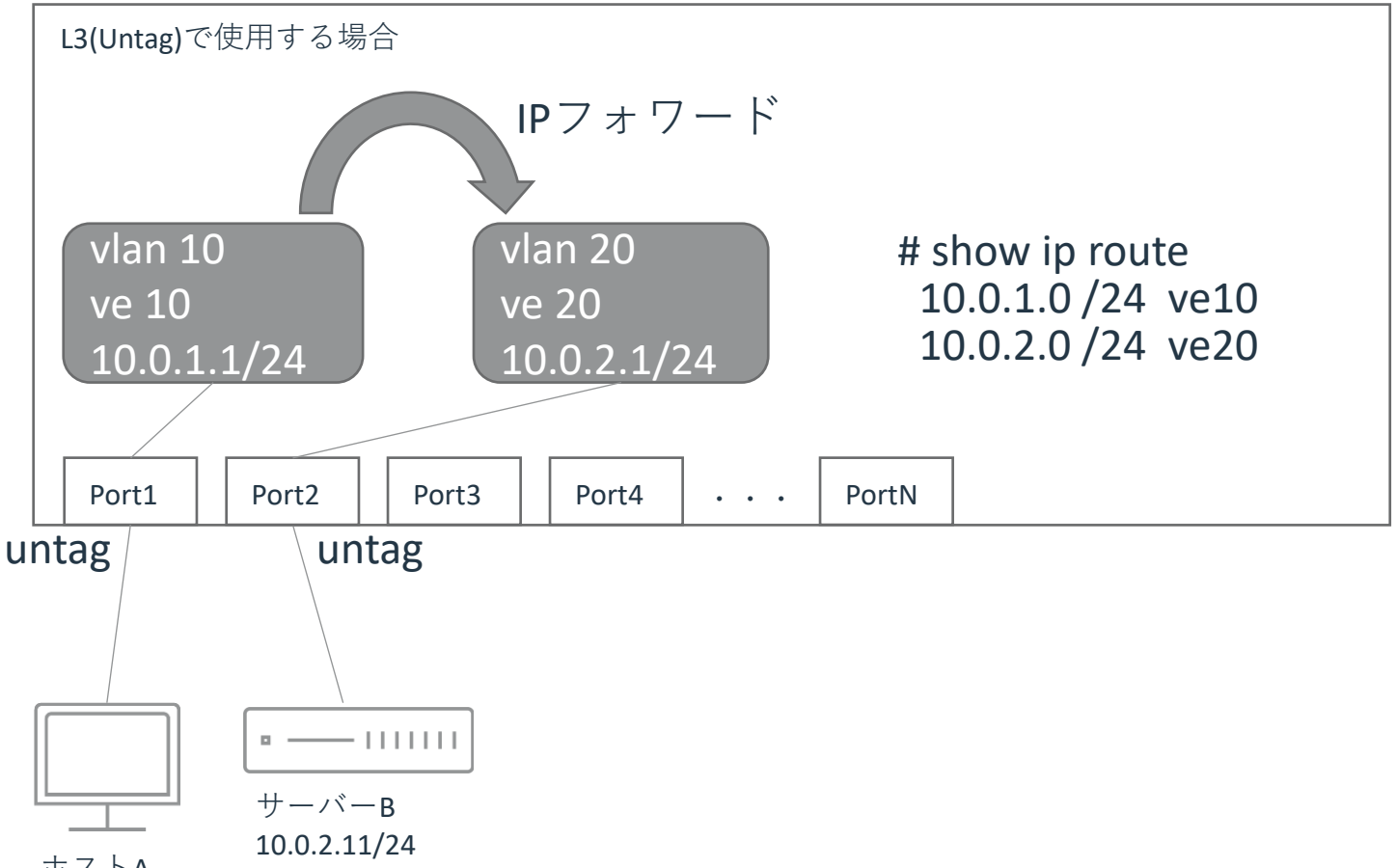
以下のように設定します。




```
A10(config)#vlan 10
A10(config-vlan:10)#untagged ethernet 1
A10(config-vlan:10)#untagged ethernet 2
A10(config-vlan:10)#exit
A10(config)#
A10(config)#vlan 20
A10(config-vlan:20)#untagged ethernet 3
A10(config-vlan:20)#untagged ethernet 4
A10(config-if:ve:20)#exit
A10(config)#
```

[補足]vlanインターフェイス(L3で使用する場合)

以下のように設定します。




```
A10(config)#vlan 10
A10(config-vlan:10)#untagged ethernet 1
A10(config-vlan:10)#router-interface ve 10
A10(config)#interface ve 10
A10(config-if:ve:10)#ip address 10.0.1.1 /24
A10(config)#
A10(config)#vlan 20
A10(config-vlan:10)#untagged ethernet 2
A10(config-vlan:10)#router-interface ve 20
A10(config)#interface ve 20
A10(config-if:ve:10)#ip address 10.0.2.1 /24
```

[補足]インターフェイス(tag/untag)

IEEE802.1Qの規格でtagをつけて使用します。
Tag付きで使用されるポートをタグVlan
またはトランクポートと呼び、
Tagなしで使用するポートをタグなしVlan、
またはアクセスポートと呼びます。

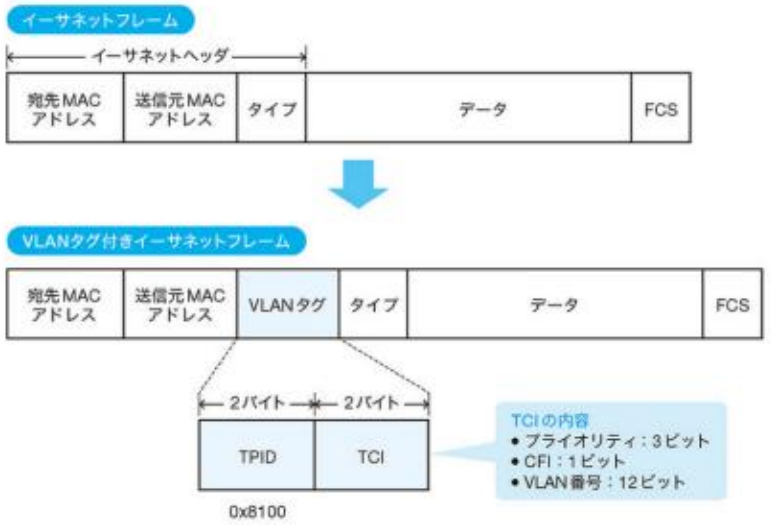
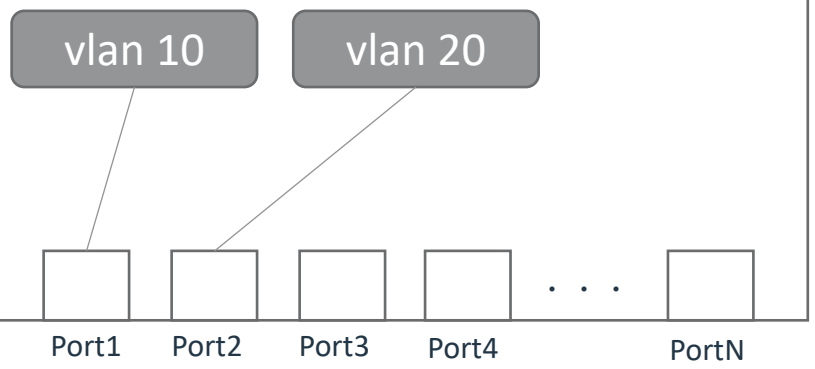
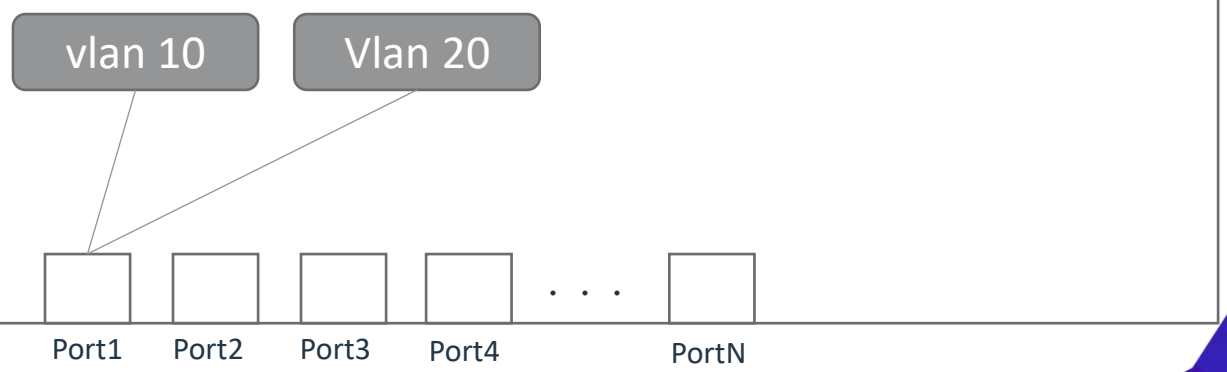


図3-10　IEEE802.1Q VLANタグ

tagなしでポートを使用する場合は各ポートは一つのVLANにしか所属することができません。

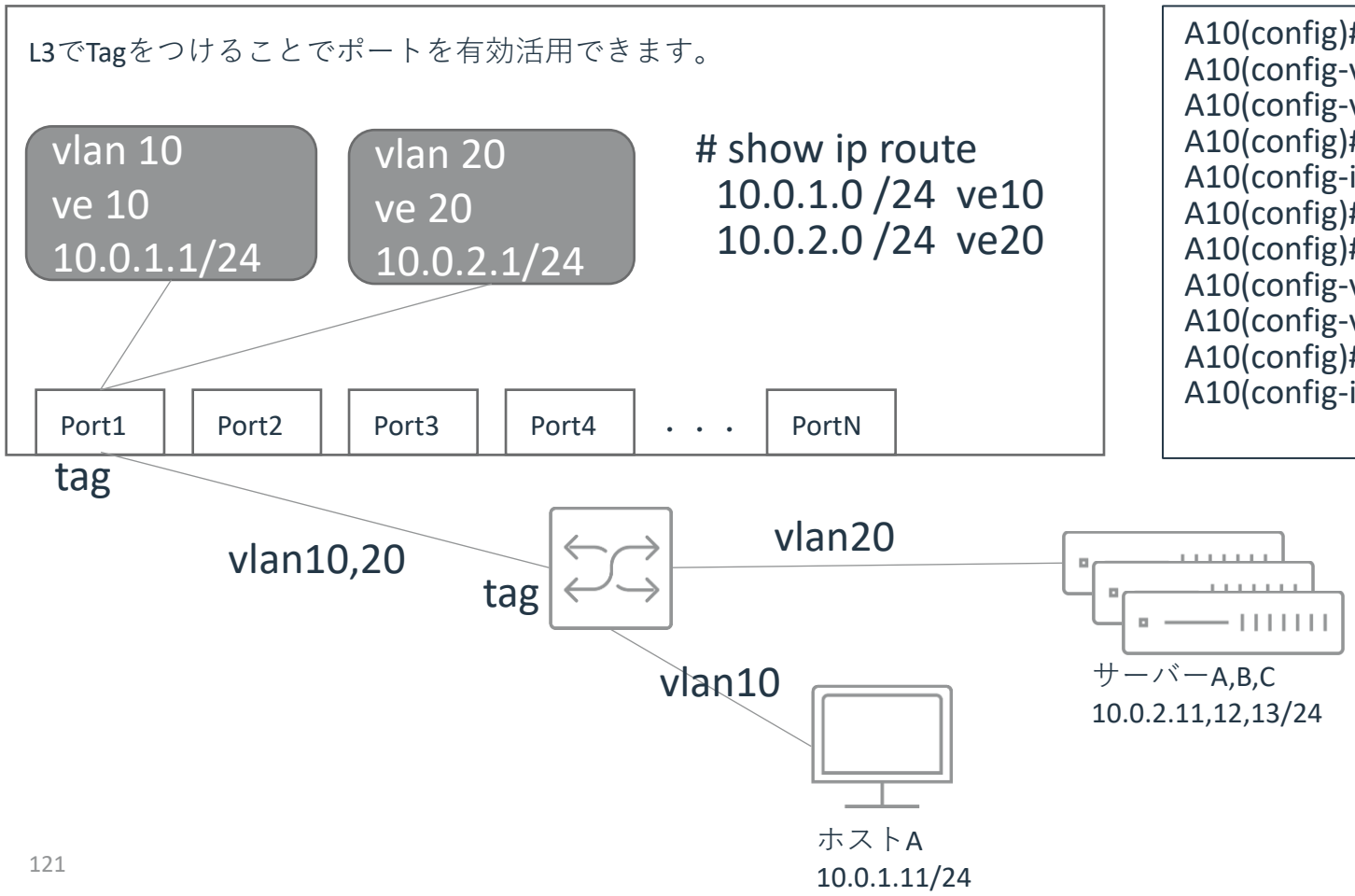


tagありでポートを使用する場合、以下のように**ポート1をVlan10とVlan20**で共有することができます。よって、物理ポートを有効活用することができます。



[補足]インターフェイスの設定(vlan)

A10でインターフェイスを使うときは以下のように設定します。

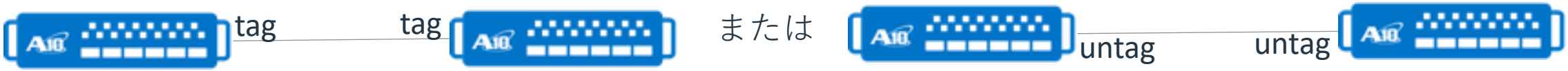



```
A10(config)#vlan 10
A10(config-vlan:10)#tagged ethernet 1
A10(config-vlan:10)#router-interface ve 10
A10(config)#interface ve 10
A10(config-if:ve:10)#ip address 10.0.1.1 /24
A10(config)#
A10(config)#vlan 20
A10(config-vlan:10)#tagged ethernet 1
A10(config-vlan:10)#router-interface ve 20
A10(config)#interface ve 20
A10(config-if:ve:10)#ip address 10.0.2.1 /24
```

[補足] タグVLANで接続するとき

使い方として

tag（またはトランクポート）は基本的には**tag（またはトランクポート）同士で接続**します。
Untagはuntag同士で接続します。



A10を使用する時、大抵は VLAN 対応スイッチ同士を接続するのですが
VLAN 非対応の PC やスイッチに接続するときは基本的には**untag （またはアクセスポート）で接続**します

ベンダーによってはVLANの設定がないPCやサーバーと、tagVlanでもNative VLAN だけには接続できるものがあります。NativeVlanとはvlan設定していないときのデフォルトのvlan IDになります。A10の場合はvlan 1がNative Vlanになるのですが、vlan 1 は使用することができません。制限事項を次のページに記載します。

[補足] Vlan A10制限事項

A10におけるVLAN設定の制限概要は次のとおりです。

- タグなしインターフェイスは1つのVLANのメンバーにしかなれません。
- １つのインターフェイスをVLANでタグなしとタグ付きの両方としては使用できません。
- VLAN1はタグ付き、またはタグなしとして設定できません。
- ネイティブVLANは設定できません。
- タグなしフレームがタグ付きインターフェイスで受信された場合はドロップされます。

付録２：トラブルシューティング

仕様確認・障害対応のフロー

ACOSのロギング

ローカルロギング

イベントログ:ハードウェアの異常、ACOSの異常、ACOS上のイベントをログに出力

show log

監査ログ:ACOSで行われたコマンドの履歴を表示

show audit

外部ロギング

splunk，rsyslogなどへの出力

```
ACOS(config)#logging host ?
  Hostname or A.B.C.D  Remote syslog host DNS name or ip address
  A:B:C:D:E:F:G:H      Remote syslog host ipv6 address
```

ログと監査(audit)ログの関連付け

標準のincludeおよびsectionユーティリティを使用して、ログ、監査ログ、実行中のconfigの対応する行を検索

```
ACOS#show log
   Sep 24 2013 09:56:45 Warning [ACOS]:Duplicated IP 10.0.1.1 MAC 000c.2976.5904
   from Port 1 VLAN 3 detected
ACOS# show audit | inc Sep 24 2013 09:56
   Sep 24 2013 09:56:46  [admin] cli:port 80 http
   Sep 24 2013 09:56:28  [admin] cli:slb virtual-server vip1 10.0.1.1
ACOS(config)#show run | sec 10.0.1.1
   ip route 0.0.0.0 /0 10.0.1.1
   slb virtual-server vip1 10.0.1.1
      port 80  http
```

ログ

Thunderは、多くの情報メッセージ、警告メッセージ、エラーメッセージをログに記録。

- ポート/インターフェイスのアップ/ダウンメッセージ
- L2ループ検出の警告
- ユニキャスト/マルチキャスト/ブロードキャストパケット制限の警告
- MACアドレス移動の警告
- 重複するIPの警告
- サーバー&サービスポートのアップ/ダウンメッセージ
- アプリケーション固有のエラーメッセージ：SLB、PBSLB、HTTP、HA、AFLEX, […]

ACOSモニタしきい値

ACOS - モニタされている使用率しきい値の確認

```
ACOS#show monitor
    Current system monitoring threshold:（デフォルト値の表示）
    Hard disk usage:85
    Memory usage:95
    Control CPU usage:90
    Data CPU usage:90
    IO Buffer usage:91750
    Buffer Drop:4000
    Warning Temperature: 68
    […]
```

レイヤ1～4

レイヤ1～2

```
ACOS#show int
ACOS#show mac-address-table
```

レイヤ3

```
ACOS#show arp
ACOS#show ip route
```

レイヤ4

```
ACOS#telnet <ip> <port>
ACOS#axdebug
```

※ここでは基本的なものを記載。

ACOSのリソース

メモリ使用率の表示

```
ACOS#show memory [ system ]
```

```
System Memory Usage:
Total(KB)   Free        Shared      Buffers     Cached      Usage
16456546    8224340     0           2420        159084      49.0%
```

CPU使用率の表示

```
ACOS#show cpu
```

```
ACOS#repeat 1 show cpu
```

↑過去1秒, 5秒, 10秒, 30秒, 60秒間の各cpu使用率を表示。
「repeat」コマンドを先頭につけることによって連続的に実行できる。

リソース制限の表示

```
ACOS#show system resource-usage
```

↑システム設定, セッションキャパシティの最小、最大、デフォルトおよび現在設定されている制限値を表示

```
ACOS#show slb resource-usage
```

↑SLB設定アイテムの最小、最大、デフォルトおよび現在設定されている制限値を表示

パケットキャプチャ（axdebug）

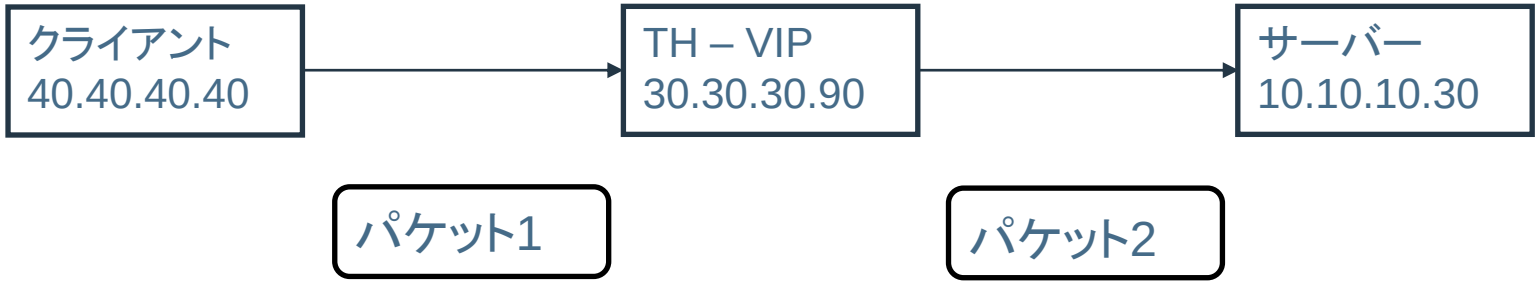
axdebug

キャプチャされたファイルはpcap形式（Wireshark / tcpdump)

Thunderから入出力されるパケットのすべての詳細を表示可能

axdebugはセッションベース

1つのパケットがフィルタに一致すると、同一セッション内の以降のすべてのパケットがダンプされる。



axdebugフィルタ

キャプチャを微調整するフィルタを構築

フィルタ内の複数の条件をANDで結合し、複数のフィルタをORで結合

axdebugの例

〇Axdebugモード起動

```
ACOS#axdebug
```

〇フィルタの作成

```
ACOS(axdebug)#filter 1
ACOS(axdebug-filter:1)#ip 1.2.3.4 /32
```

〇トレースの開始

```
ACOS(axdebug)#capture brief save <file_name>
```

〇トレースの停止

“brief”オプションを使用する場合 “Ctl+C “でキャプチャの停止

“brief”オプションを使用しない場合 “ACOS#no axdebug”でキャプチャの停止

Axdebug Capture Brief

```
vth01-Active(axdebug)#cap br
Wait for debug output, enter <ctrl c> to exit
@4358256239 i( 1,  11)> ip 192.168.0.10 > 192.168.1.101 tcp  56470 > 80 S f69a87f7:0(0) <mswt, m=1460,w=7>
@4358256239 o( 1,   0)> ip 192.168.1.101 > 192.168.0.10 tcp  80 > 56470 SA 188fe976:f69a87f8(0) <mswt, m=1460,w=2>
@4358256239 i( 1,  11)> ip 192.168.0.10 > 192.168.1.101 tcp  56470 > 80 A f69a87f8:188fe977(0)
@4358256239 i( 1,  11)> ip 192.168.0.10 > 192.168.1.101 tcp  56470 > 80 PA f69a87f8:188fe977(77)
@4358256239 o( 2,   0)> ip 192.168.2.253 > 192.168.2.10 tcp  28466 > 80 S b55e7f3a:0(0) <mswt, m=1460,w=2>
<省略>
vth01-Active(axdebug)#
```

@4358256239 **i(1, 11)> ip 192.168.0.10 > 192.168.1.101 tcp 56470 > 80 PA** f69a87f8:188fe977(77)

i
トラフィックの方向: i (input) 、 o (output)
(1, 11)
1　ポート番号
11　vlanのID
ip 192.168.0.10 > 192.168.1.101
ip Etherタイプ(ip/arp/ipv6)
192.168.0.10 送信元IP
192.168.1.10 宛先IP

tcp
L4プロトコルパケット(tcp/udp/icmp)
56470 > 80
56470 送信元ポート
80 宛先ポート
PA
TCPのフラグ:
S(Syn), SA(Syn Ack), A(Ack), F(Fin), PA(Push Ack)

axdebugファイルのエクスポート

axdebugで取得したファイルの確認

```
TH08#sh axdebug file
---------------------------------+-------------+--------------------------
Filename                         |Size(Byte) | Date
---------------------------------+-------------+--------------------------
UUU2                             |       2214 | Mon Feb  3 21:16:31 2020
fwudp                            |       2848 | Thu Dec 26 15:45:55 2019
```

axdebugトレースのエクスポート

※GUIからダウンロードも可能

```
ACOS#export axdebug <filename> [use-mgmt-port] <destination>
```

例:

```
TH08#export axdebug UUU2 scp://10.255.221.253/tmp/
User name []?root
Password []?
```

axdebugその他

パケットキャプチャの条件

デフォルトではパケット数は3000、キャプチャ時間は300秒に設定されているのでキャプチャは**自動で停止します**。変更する場合は以下のようにtimeout と count コマンドを使用します。“0”と設定するとパケットは1CPUにつき最大300MByteまでキャプチャされます。キャプチャファイルの数は最大100です。(例： タイムアウト値 600秒、パケット数 10000 に変更)

```
ACOS(axdebug)#timeout 600

ACOS(axdebug)#count 10000

ACOS(axdebug)#capture brief save <file_name>
```

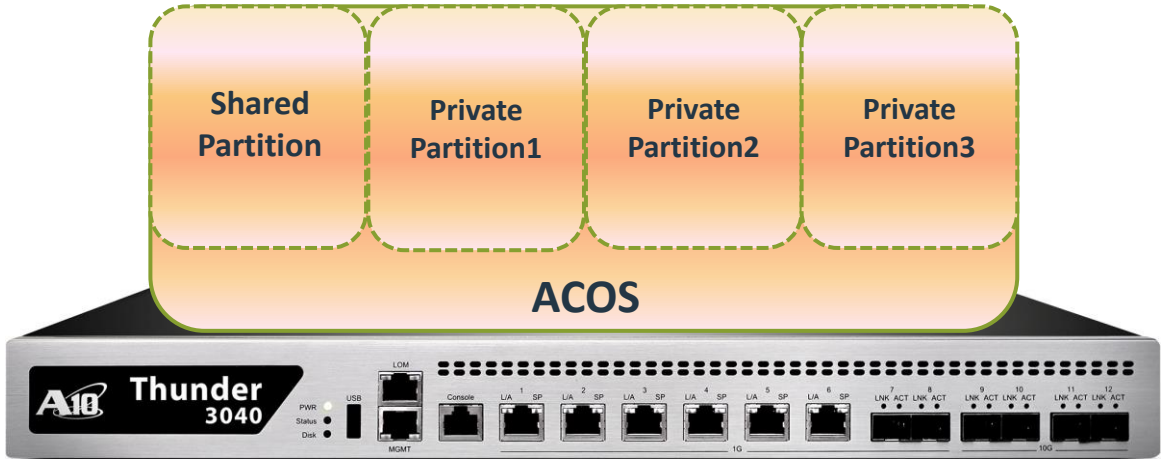
axdebugのステータス確認

```
ACOS#sh axdebug status
axdebug is disabled <=キャプチャ状態か否かを確認
session filter is enabled
…
ACOS#
```

付録３：仮想化機能
ADP(Application Delivery Partition)

ADP(Application Delivery Partition)とは

- **ADPはACOSが提供する仮想化機能**
  - 1台のThunder(1つのACOS)上に複数の仮想インスタンスを作成
    - 作成できるインスタンスの数は製品モデルによって異なる。
  - Thunderは仮想インスタンスをPartitionとして提供
    - **Shared Partition :** デフォルトPartition (ADP未使用時点のThunderそのもの)
    - **Private Partition :** Shared Partitionで追加作成するPartition(仮想インスタンス)



Thunderシリーズ

ADP：サポートされるPartition数

TABLE 7 : Supported Number of L3V Partitions per Device

Device	*Maximum Number of L3V Partitions Supported*
THUNDER SERIES	
Thunder 14045 (FTA)	1023
Thunder 7650 (FTA)	1023
Thunder 7445(S) (FTA)	1023
Thunder 7440(S)-11 (FTA)	1023
Thunder 7440(S) (FTA)	1023
Thunder 6635(S) (FTA)	1023
Thunder 6630(S) (FTA)	1023
Thunder 6440(S) (FTA)	1023
Thunder 6435(S) (FTA)	1023
Thunder 6430(S) (FTA)	1023
Thunder 5845(S) (FTA)	1023
Thunder 5840(S)-11 (FTA)	1023
Thunder 5840(S) (FTA)	1023
Thunder 5650(S)	1023
Thunder 5630(S) (FTA)	1023

TABLE 7 : Supported Number of L3V Partitions per Device (Continued)

Device	*Maximum Number of L3V Partitions Supported*
Thunder 5440(S) (FTA)	1023
Thunder 5435(S) (FTA)	1023
Thunder 5430(S)-11 (FTA)	1023
Thunder 5330S (FTA)	127
Thunder 4440(S) (FTA)	127
Thunder 4435(S) (FTA)	127
Thunder 4430S (FTA)	127
Thunder 3430(S) (FTA)	127
Thunder 3350 (Non-FTA)	127
Thunder 3230S (FTA)	64
Thunder 3030S (Non-FTA)	64
Thunder 1040S (Non-FTA) 16G memory	64
Thunder 1040/1040S (Non-FTA) 8G memory	32
Thunder 1030S (Non-FTA)	32
Thunder 930 (Non-FTA)	32
Thunder 840 (Non-FTA)	32
VIRTUAL THUNDER SERIES	
vThunder	32
AX SERIES	
AX 5630 (FTA)	1023
AX 5200 (FTA)	127
AX 3530 (Non-FTA)	127
AX 3200-12 (FTA)	64

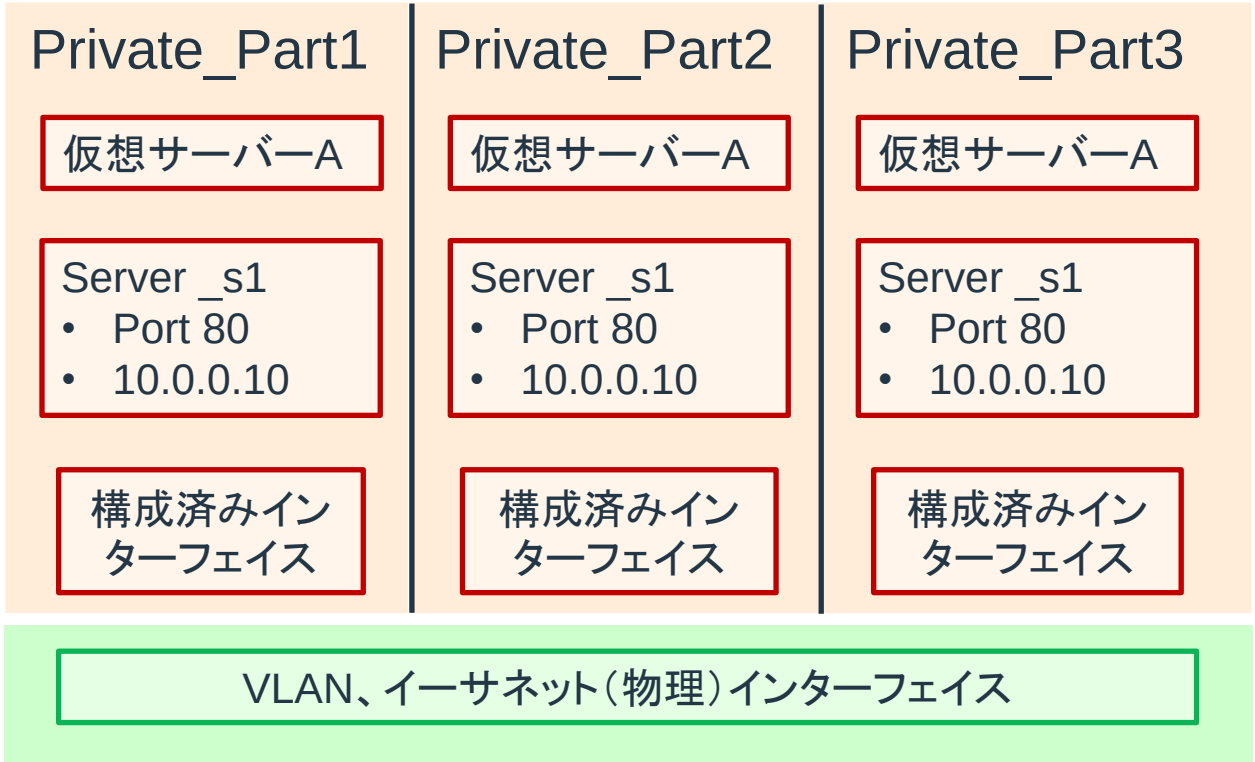
ADP: プライベートパーティションで共有されるリソース

アプリケーションデリバリーパーティション（ADP）は、

コンフィグ要素を分離し、独立して管理するための機能を提供する。

プライベート空間：レイヤ3～7

共有空間：レイヤ1～2



ADP: プライベートオブジェクトとパブリックオブジェクト

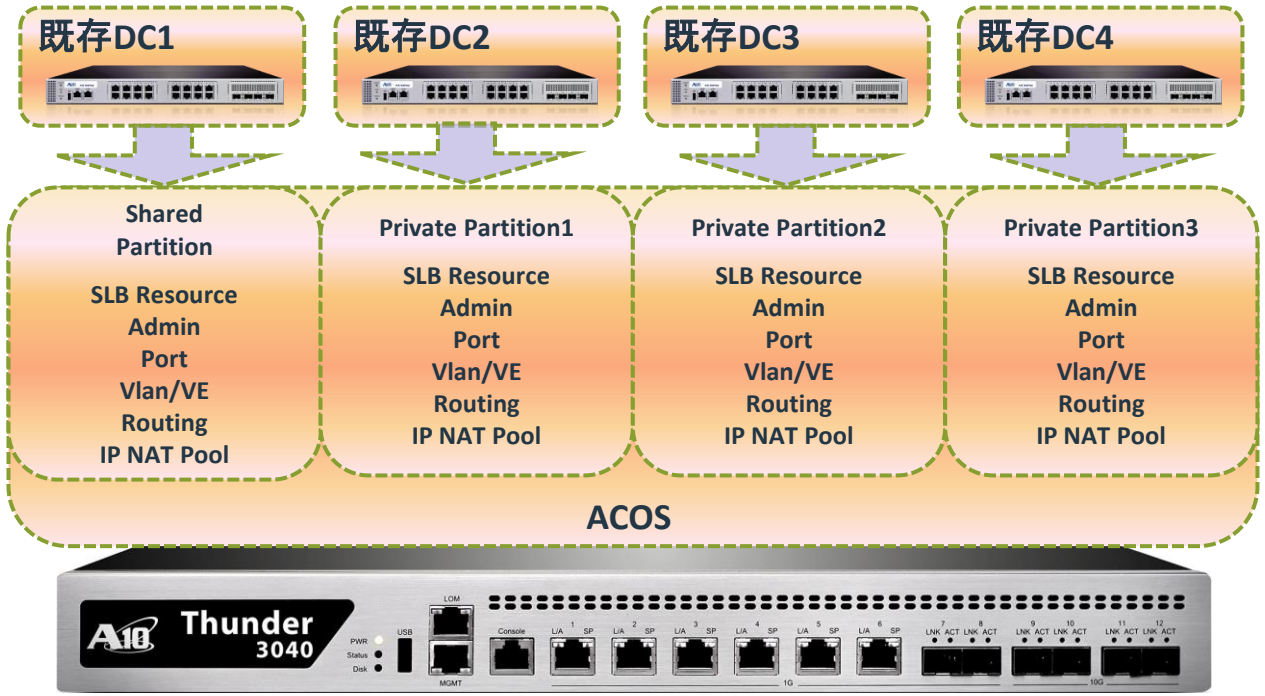
- **パブリックオブジェクト**
  - **イーサネットインターフェイス**
    - タグなしイーサネットインターフェイスは単一のパーティションからのみ使用可能
    - タグ付きイーサネットインターフェイスは複数のパーティションから使用可能
  - **VLAN**
    - VLANは、1つのパーティションによって所有されると他のパーティションでは見えなくなり、再利用はできない。

- **プライベートオブジェクト**

  仮想インターフェイス(VE)
  静的MACエントリ
  IPアドレス
  ARPエントリ
  ルーティングテーブル
  ACL
  実サーバー
  バーチャルサーバー
  サービスグループ
  テンプレート
  ヘルスモニター
  証明書と鍵
  aFleXポリシー

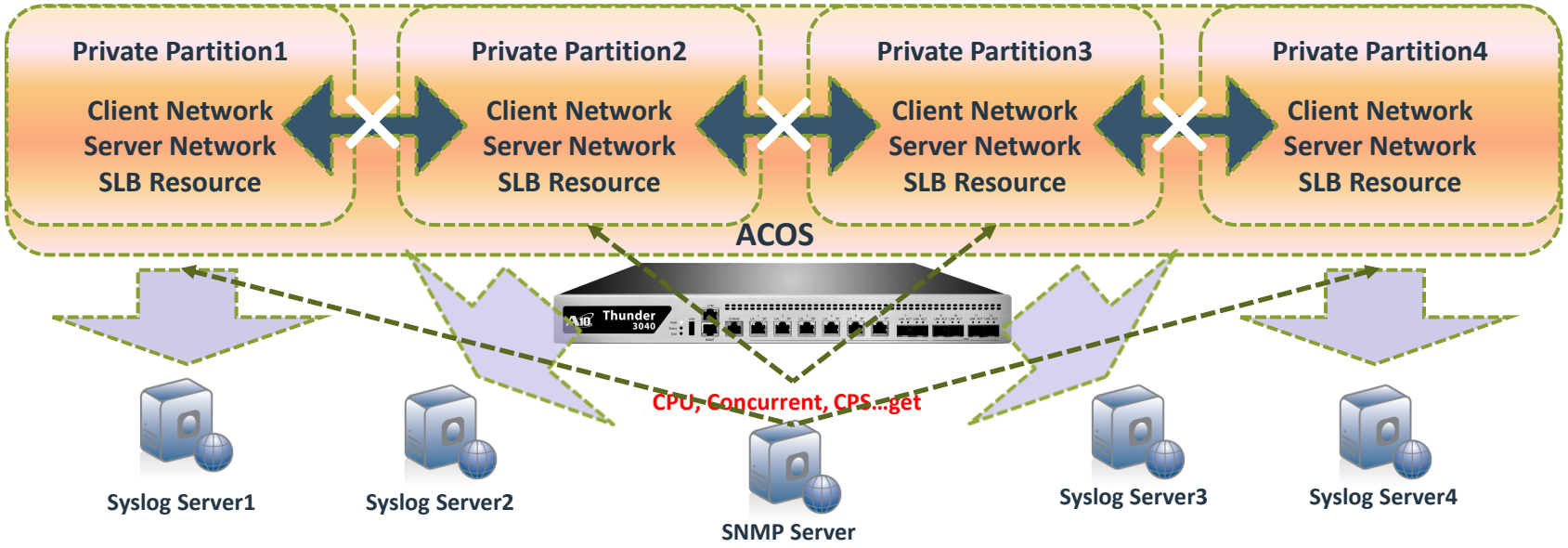
ADP: 特徴と実現できること

- 【複数Data Center, 複数システムの統合】
  - **点在するロードバランサーを1台のThunderに集約**
    - **Case:**
      - ランニングコストを削減をしたい
        - Data Center使用料、Rack使用料、電力費用、機器保守費
      - サービス拡張を簡単に行いたい、機器導入負荷/コストを削減したい
        - Partitionの追加、Partition作成をテンプレート化



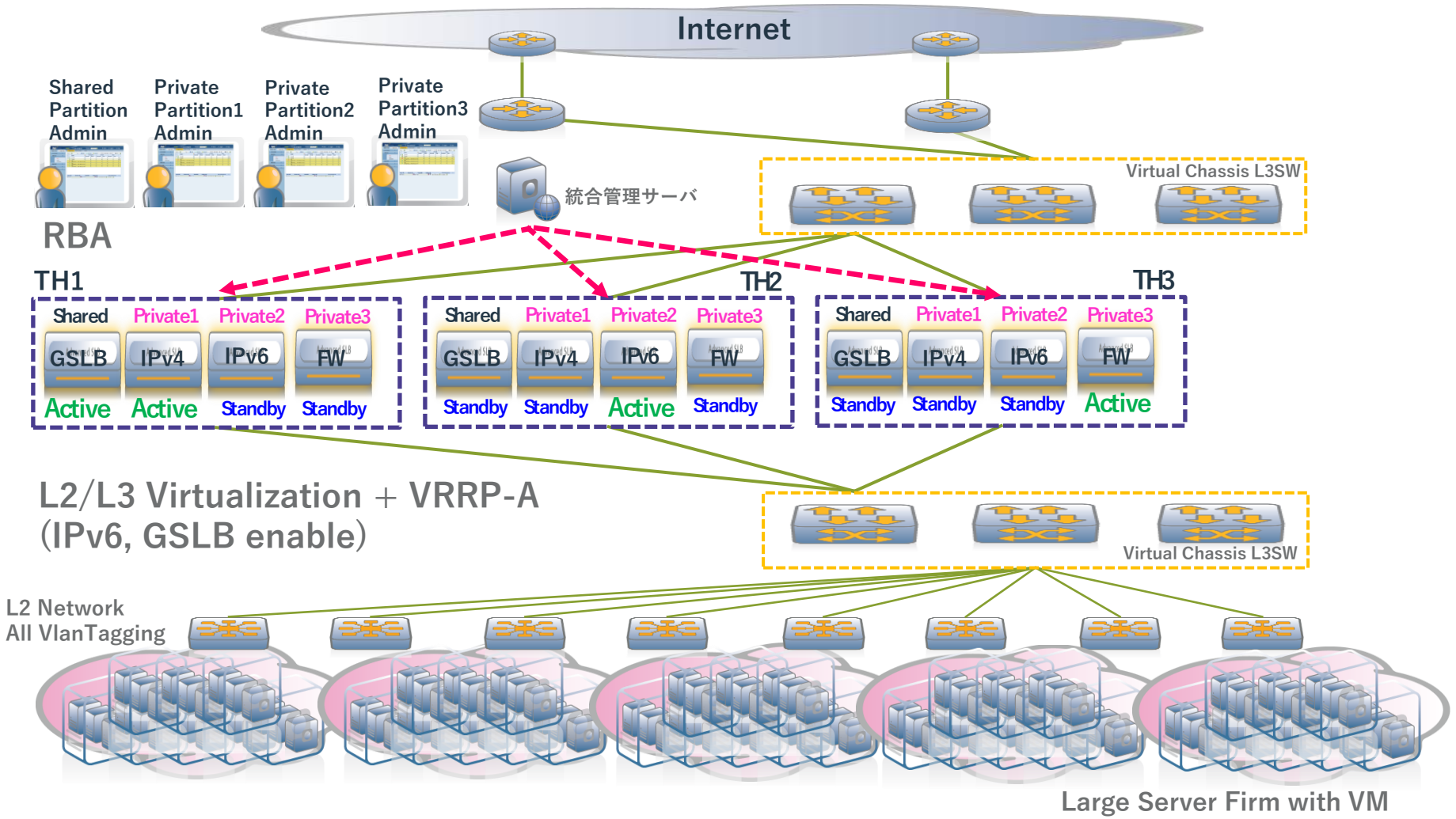
ADP:特徴と実現できること

- 【Partitionの独立性, 管理運用性の確保】
  - **Partition間の相互閲覧、相互通信不可**
    - **Case:**
      - 複数システムを1台のBoxに集約した上で、セキュリティを確保したい
  - **各PartitionをSyslog, SNMPで管理可能**
    - **Case:**
      - Partitionごとにログ管理を行いたい
      - Partition個別の情報をSNMPで取得したい



ADP:冗長構成イメージ

- ADP & VRRP-A



ADP:プライベートパーティションの作成と確認

- プライベートパーティションの作成
- A1(config:1)# partition inside id 1 [application-type <ADC|CGNV6>]

- Macアドレス重複を防止するための設定
- A1(config:1)# system promiscuous-mode #vThunderを使用しているときに必要になります。
- A1(config:1)# system ve-mac-scheme system-mac #重複防止、reloadが必要になります。

- 既存のパーティションとポートオーナーの一覧表示
- A1# **show partition**
  - Partition Name Id App Type Admin Count
  - inside 1 ADC 0
  - outside 2 ADC 0
  -

- A1-vMaster[1/1]# show partition port-ownership
  - Port 1 shared by Network partitions:
  - shared via VLAN 100
  - HELIUM via VLAN 101
  - Port 2 shared by Network partitions:
  - shared via VLAN 200
  - HELIUM via VLAN 1201
  - Port 3 shared by Network partitions:
  - shared via VLAN 300
  - HELIUM via VLAN 301

ADP:パーティション間の移動

active-partitionコマンドで、パーティション間を移動する。

- A1# active-partition ?
  shared Shared partition
  inside
  outside

- A1# **active-partition inside** //insideパーティションに移動
  Currently active partition: inside
- A1[inside]#**active-partition** shared //共有パーティションに移動
  Currently active partition: shared

ADP：コンフィグプロファイルおよびバックアップの表示

- ほとんどのコマンドは通常、パーティション内で機能する。
  - A1[inside]# **show running-config**

  例外：バックアップシステム[...]
  - A1[inside]# **export running-config use-mgmt-port <URI_remote_host_path>**

- 共有パーティションから、全パーティションのコンフィグを表示する。
  - A1# **show running-config partition-config {all|shared|NAME}**
  - A1# **show startup-config all-partitions**
  - A1# **show startup-config partition {shared|NAME}**

- 共有パーティションから、全パーティションのコンフィグを保存する。
  - A1# **write memory all-partitions**

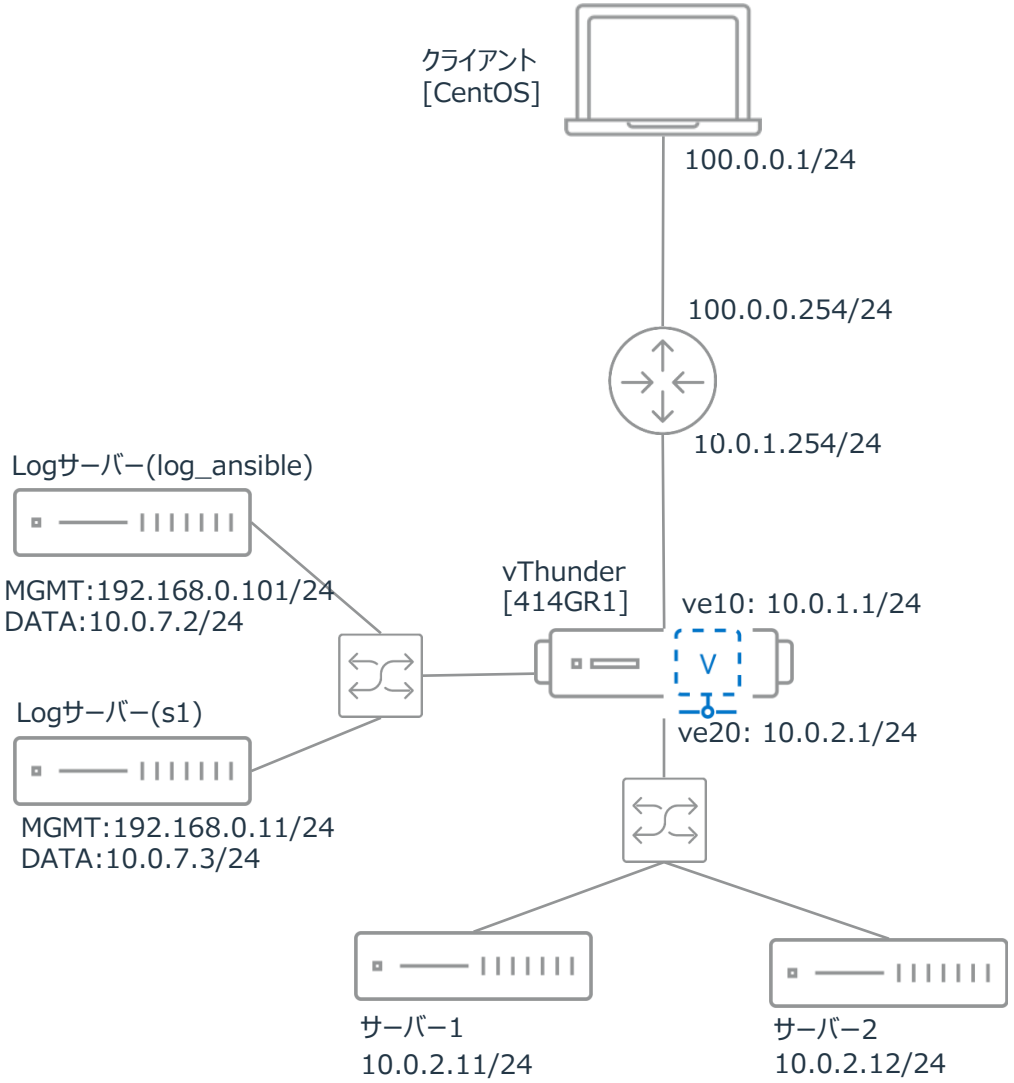
ADP：プライベートパーティションの削除

- 「no partition」コマンドにより、コンフィグからパーティションを削除。
  パーティションはデバイスに保持され、パーティションコマンドを使用して元に戻すことができる。
  - A1-vMaster[1/1](config:1)# **no partition HELIUM id 1**
  - Remove this partition and keep configurations on the disk? (y/n) **y**
  - A1-vMaster[1/1](config:1)

- 「delete partition」コマンドを使用すると、デバイスからパーティションが完全に削除される。
  パーティションは、削除する前に構成から除外する必要がある。
  パーティションは、元に戻して再構成しないとリストアできない。
  - A1-vMaster[1/1](config:1)# **no partition HELIUM id 1**
  - Remove this partition and keep configurations on the disk? (y/n) **y**
  - A1-vMaster[1/1](config:1)# **delete partition HELIUM ID 1**
  - The operation will delete this partition permanently from all profiles on disk.
  - This action is not recoverable.Continue? [yes/no]: **yes**
  - A1-vMaster[1/1](config:1)#

付録4：ログ機能

ラボネットワーク構成



Management IP	
クライアントPC:	192.168.0.100(RDP student/a10)
Log_Ansible:	192.168.0.101(SSH root/a10)
A1:	192.168.0.1/24(SSH admin/a10)
A2-DNS:	192.168.0.2/24(SSH admin/a10)
A3-FW:	192.168.0.3/24(SSH admin/a10)
A4-WEB:	192.168.0.4/24(SSH admin/a10)
A5-Router-Proxy:	192.168.0.5/24(SSH admin/a10)
サーバー1:	192.168.0.11/24(SSH root/a10)
サーバー2:	192.168.0.12/24(SSH root/a10)

ログ設定について

ACOSログは大きくは2種類あります。
(詳細はマニュアルA10_4.1.4-GR1-P5_SAG, A10_4.1.4-GR1-P5_ELOGを参照)

1．イベントログ
　　設定方法は「logging host xxx.xxx.xxx.xx」または「ACOS-EVENT(推奨)」の２種類あります。
　　ログを複数のサーバーに出力することができます。

2．Auditログ(A10の操作履歴)
　　設定方法は「logging auditlog host xxx.xxx.xxx.xxx facility localx」と１種あります。
　　Auditログに関しては414gr1p5で使用できるログサーバーは１台です。

ログ設定の推奨構成について

1．ACOS-EVENTでログ設定をする。

ACOS-EVENTではログデータを負荷分散してサーバーに送信する方式と
同じログを複数のサーバーに送信する方式の2種類を設定することができます。
また、FWログ等もACOS-EVENT機能に統合されています。

2．ログ出力はデータポート経由で行う。

ログ出力はマネジメント、データポート両方より可能ですが
FWセッションログ等、セッションに関するログは
マネジメントポートから出力できないものがあります。

3．複数ログサーバーを使用する場合、同じログを各サーバーに出力することを推奨。

運用上、ログが異なるサーバーに分散されると
ログ検索・トラッキングが困難です。

ログ設定の特徴(ACOS-Event)

■複数のログサーバーへのログ出力方法

○ 同じログを複数のサーバーに出力する場合、
　２つのcollector-group を作成して負荷分散します。

○複数のサーバーにログを負荷分散して出力する場合、
　1つのcollector-group に２つのログサーバーを設定します。

ACOS-Event(設定):複数サーバーへ同一ログ配信

```
interface ethernet 7
  enable
  ip address 10.0.7.1 255.255.255.0
!
acos-events message-selector ms1
  rule 1
    message-id cmroot all
!
acos-events log-server aelog1 10.0.7.2
    port 514 udp
    health-check-disable
!
acos-events log-server aelog2 10.0.7.3
   port 514 udp
    health-check-disable
!
acos-events collector-group cg1 udp
  log-server aelog1 514
!
acos-events collector-group cg2 udp
  log-server aelog2 514
!
acos-events template aetemp1
  message-selector ms1
    collector-group cg1
    collector-group cg2
!
acos-events active-template aetemp1
```

- データネットワーク経由でログ出力します。
- 複数のcollector-groupにそれぞれ1つのログサーバーを設定します。

```
[ExplicitProxyのときはポリシーテンプレートに設定]
slb template policy policy01
  forward-policy
    acos-event-log
    action F2I
        forward-to-internet ep1 snat natp1
        log
```

ACOS-Event(ログ出力サンプル)

- 複数サーバーへ同一ログ送信

ログサーバー０１

```
Mar 16 14:14:53 A10 a10lb: [ACOS]<6> result=SUCCESS, client-ip=100.0.0.1, client-port=36726, server-ip=10.0.2.11, server-port=80, snat-ip=10.0.3.211, snat-port=2054, host=www.office365.me, request-method=GET, request=http://www.office365.me/, bytes=133, action=To Internet, policy=cloud-app-template, source-rule=client-ip-to-proxy, destination-priority=990, virtual-server=v1, virtual-server-port=8080
Mar 16 14:14:53 A10 a10lb: [ACOS]<6> result=SUCCESS, client-ip=100.0.0.1, client-port=36726, server-ip=10.0.2.11, server-port=80, snat-ip=10.0.3.211, snat-port=2054, response-code=200, bytes=446, action=From Internet, policy=cloud-app-template, source-rule=client-ip-to-proxy, destination-priority=990, virtual-server=v1, virtual-server-port=8080
Mar 16 14:17:30 A10 a10logd: [ACOS]<6> Ethernet interface 1 is down
Mar 16 14:17:30 A10 a10logd: [ACOS]<6> Virtual Ethernet interface ve10 is down
Mar 16 14:17:32 A10 a10logd: [ACOS]<6> Virtual Ethernet interface ve10 is up
Mar 16 14:17:32 A10 a10logd: [ACOS]<6> Ethernet interface 1 is up
```

ログサーバー０２

```
Mar 16 14:14:53 A10 a10lb: [ACOS]<6> result=SUCCESS, client-ip=100.0.0.1, client-port=36726, server-ip=10.0.2.11, server-port=80, snat-ip=10.0.3.211, snat-port=2054, host=www.office365.me, request-method=GET, request=http://www.office365.me/, bytes=133, action=To Internet, policy=cloud-app-template, source-rule=client-ip-to-proxy, destination-priority=990, virtual-server=v1, virtual-server-port=8080
Mar 16 14:14:53 A10 a10lb: [ACOS]<6> result=SUCCESS, client-ip=100.0.0.1, client-port=36726, server-ip=10.0.2.11, server-port=80, snat-ip=10.0.3.211, snat-port=2054, response-code=200, bytes=446, action=From Internet, policy=cloud-app-template, source-rule=client-ip-to-proxy, destination-priority=990, virtual-server=v1, virtual-server-port=8080
Mar 16 14:17:30 A10 a10logd: [ACOS]<6> Ethernet interface 1 is down
Mar 16 14:17:30 A10 a10logd: [ACOS]<6> Virtual Ethernet interface ve10 is down
Mar 16 14:17:32 A10 a10logd: [ACOS]<6> Virtual Ethernet interface ve10 is up
Mar 16 14:17:32 A10 a10logd: [ACOS]<6> Ethernet interface 1 is up
```

ACOS-Event(設定):ログサーバー負荷分散

```
interface ethernet 7
  enable
  ip address 10.0.7.1 255.255.255.0
!
acos-events message-selector ms1
  rule 1
    message-id cmroot all
!
acos-events log-server aelog1 10.0.7.2
    port 514 udp
    health-check-disable
!
acos-events log-server aelog2 10.0.7.3
   port 514 udp
    health-check-disable
!
acos-events collector-group cg1 udp
  log-server aelog1 514
  log-server aelog2 514
!
acos-events template aetemp1
  message-selector ms1
    collector-group cg1
!
acos-events active-template aetemp1
!
```

- データネットワーク経由でログ出力します。
- １つのcollector-groupに複数のログサーバーを設定します。

[ExplicitProxyのときはポリシーテンプレートに設定]

```
slb template policy policy01
  forward-policy
    acos-event-log
    action F2I
        forward-to-internet ep1 snat natp1
        log
```

ACOS-Event(ログ出力サンプル)

- ログサーバ負荷分散

ログサーバー０１

Mar 16 14:01:10 A10 a10lb: [ACOS]<6> result=SUCCESS, client-ip=100.0.0.1, client-port=35478, server-ip=10.0.2.11, server-port=80, snat-ip=10.0.3.211, snat-port=2052, host=www.office365.me, request-method=GET, request=http://www.office365.me/, bytes=133, action=To Internet, policy=cloud-app-template, source-rule=client-ip-to-proxy, destination-priority=990, virtual-server=v1, virtual-server-port=8080
Mar 16 14:04:14 A10 a10logd: [ACOS]<6> Virtual Ethernet interface ve10 is down
Mar 16 14:04:16 A10 a10logd: [ACOS]<6> Ethernet interface 1 is up

ログサーバー０２

Mar 16 14:01:10 A10 a10lb: [ACOS]<6> result=SUCCESS, client-ip=100.0.0.1, client-port=35478, server-ip=10.0.2.11, server-port=80, snat-ip=10.0.3.211, snat-port=2052, response-code=200, bytes=446, action=From Internet, policy=cloud-app-template, source-rule=client-ip-to-proxy, destination-priority=990, virtual-server=v1, virtual-server-port=8080
Mar 16 14:04:14 A10 a10logd: [ACOS]<6> Ethernet interface 1 is down
Mar 16 14:04:16 A10 a10logd: [ACOS]<6> Virtual Ethernet interface ve10 is up

ACOS-Event(設定) フォーマット変更

```
acos-events collector-group cg1 udp
 format cef     //書かなければデフォルトsyslogフォーマット
 log-server aelog1 514
```

- CEF

```
Dec 28 13:06:04 2020 A1  CEF:0|A10|CFW|4.1.4-GR1-P3|FW 101|Session closed|1|proto=TCP act=Permit rt=2202292 src=10.0.0.2 spt=56070 dst=172.16.0.2 dpt=80 deviceInboundInterface=ve10 deviceOutboundInterface=ve20 cs1=fw-r1 cs2=rule-web cs3=Client initiated in=629 out=478 cn1=6 cn2=4 cn3=2 cs1Label=Rule Set Name cs2Label=Rule Name cs3Label=Reason cn1Label=Packets TX cn2Label=Packets RX cn3Label=Session Duration Seconds

Dec 28 13:06:05 2020 A1  CEF:0|A10|CFW|4.1.4-GR1-P3|FW 101|Session closed|1|proto=TCP act=Permit rt=2202472 src=10.0.0.2 spt=56072 dst=172.16.0.2 dpt=80 deviceInboundInterface=ve10 deviceOutboundInterface=ve20 cs1=fw-r1 cs2=rule-web cs3=Client initiated in=629 out=478 cn1=6 cn2=4 cn3=2 cs1Label=Rule Set Name cs2Label=Rule Name cs3Label=Reason cn1Label=Packets TX cn2Label=Packets RX cn3Label=Session Duration Seconds
```

Auditログ

AuditログはA10の操作履歴です。

logging auditlog host 10.0.7.2 facility local0

10.0.7.2 ：SyslogサーバーのIPアドレス
facility：Facility設定はログの種類を表します。 local0からlocal7で任意のものを設定してください。

出力サンプル

```
Mar 16 11:50:32 A10 a10logd: [audit log]<6>  [admin] cli: [192.168.0.100:38656] show slb server
Mar 16 11:53:05 A10 a10logd: [audit log]<6>  [admin] cli: [192.168.0.100:38656] show running-config logging
Mar 16 11:53:10 A10 a10logd: [audit log]<6>  [admin] cli: [192.168.0.100:38656] configure
Mar 16 11:53:17 A10 a10logd: [audit log]<6>  [admin] cli: [192.168.0.100:38656] logging auditlog host 10.0.7.2 facility local7
Mar 16 11:54:19 A10 a10logd: [audit log]<6>  [admin] cli: [192.168.0.100:38656] show running-config logging
Mar 16 12:14:54 A10 a10logd: [audit log]<6>  [admin] cli: [192.168.0.100:38656] configure
Mar 16 12:15:06 A10 a10logd: [audit log]<6>  [admin] cli: [192.168.0.100:38656] logging auditlog host 192.168.0.11 facility local7
Mar 16 12:15:19 A10 a10logd: [audit log]<6>  [admin] cli: [192.168.0.100:38656] show version
Mar 16 12:15:21 A10 a10logd: [audit log]<6>  [admin] cli: [192.168.0.100:38656] show log
Mar 16 12:28:50 A10 a10logd: [audit log]<6>  [admin] cli: [192.168.0.100:38656] show running-config logging
Mar 16 12:33:36 A10 a10logd: [audit log]<6>  [admin] cli: [192.168.0.100:38656] logging auditlog host 192.168.0.11 facility local0
Mar 16 12:33:54 A10 a10logd: [audit log]<6>  [admin] cli: [192.168.0.100:38656] show version
```