IBM SevOne NPM NPM 設定ガイド
3. ネットワーク監視

2022年6月10日
日本アイ・ビー・エム株式会社
データ・AI・オートメーション事業部

© 2022 IBM Corporation

はじめに

■ 当資料の位置づけ

– 当資料は、IBM SevOne Network Performance Management (NPM) ソリューションのうち、Data Appliance NMS (PAS) とData Insightの構成およびこれらを使用した基本的な監視機能についての動作確認結果を設定ガイドとしてまとめたものです。SevOneの全機能、もしくはそれらの組み合わせを網羅した資料ではありません。

■ 注意事項

– 当資料に含まれる情報は可能な限り正確を期しておりますが、正式なレビューを受けておらず、当資料に記載された内容に関して何ら保証するものではありません。ここでの記載内容はあくまでも支援情報であり、使用者の責任において取扱われるものとし、資料の内容によって受けたいかなる損害に関して一切の保証をするものではありません。

■ 変更履歴

– 2022年4月　　初版 (v1.0) 作成
– 2022年5月　　juniper機器の検証結果を追記

※NMS: Network Management System
※PAS: Performance Appliance System

©2022 IBM Corporation

3. ネットワーク監視

©2022 IBM Corporation

目次

©2022 IBM Corporation

3.1. SNMP

■ 検証内容

– SNMP Walk (SNMP v2c)

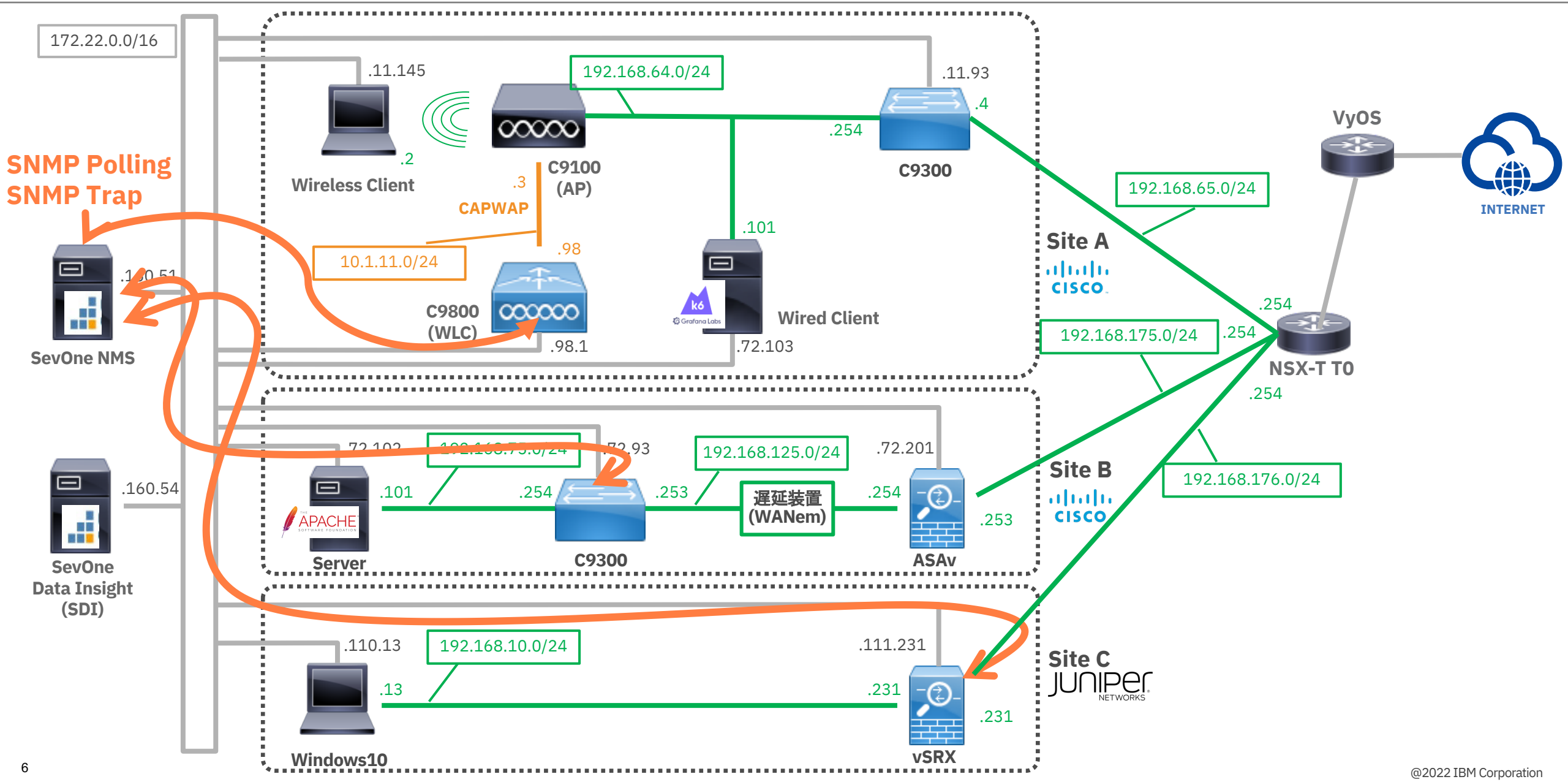
- SevOne NMSからスイッチに対してSNMP Walkを行いMIB情報を取得できることを確認する

– SNMP Trap受信 (SNMP v2c)

- スイッチにてInterface障害を発生させ、そのときのTrapがSevOne NMSで受信/処理できることを確認する

©2022 IBM Corporation

3.1.1. 検証構成



@2022 IBM Corporation

3.1.2. 設定

■ 設定概要

1. NMSの設定

- NMS Cluster Levelの設定
- NMS管理下のデバイスに対する個別のSNMP設定
- SNMP Polling監視項目の設定
- Trap受信時の挙動の設定

2. デバイスのSNMP設定

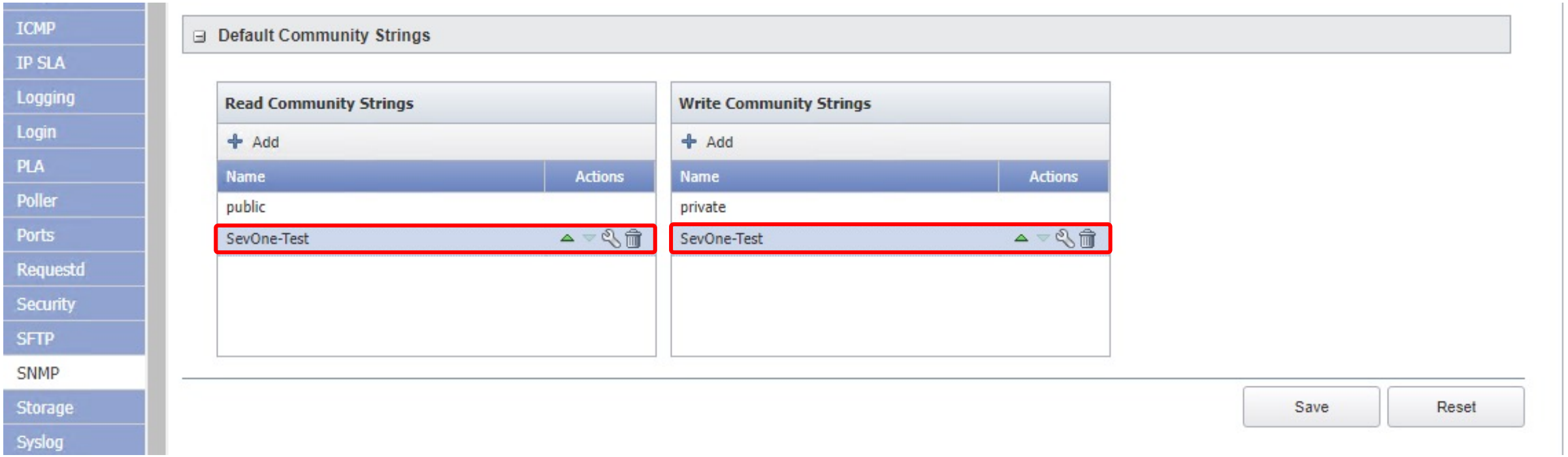
- Catalyst 9300のSample Config
- Catalyst 9800のSample Config
- vSRXのSample Config

※本資料ではC9300、C9800、vSRXでのSNMPの設定方法を紹介しているが、検証結果はC9300のみ掲載している。他の機器についても同様にSNMP Walk、SNMP Trapの動作確認を実施したが、C9300と同様の結果となったため検証結果の内容は省略している。

©2022 IBM Corporation

3.1.2.1. NMSの設定 (1/6)

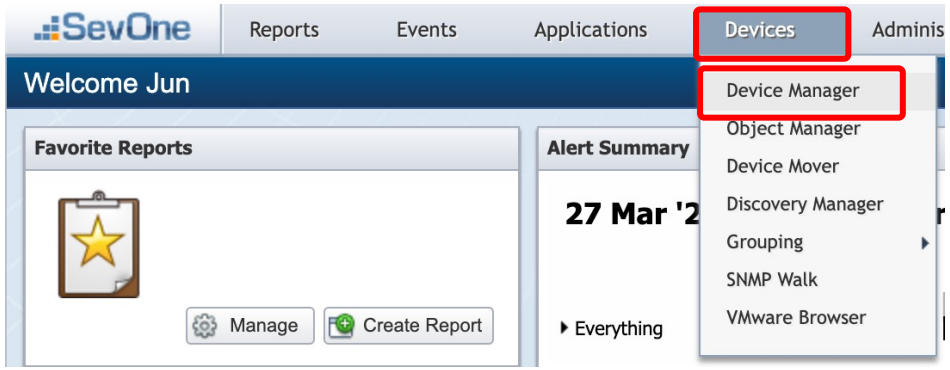
- NMS Clusterレベルでの設定
  - [Administration] > [Cluster Manager] > [Cluster Settings] > [SNMP] でClusterレベルのSNMP設定が可能
  - 本検証ではDefault Community Stringのみ設定をカスタマイズ
    - Default Community Stringは、NMSがデバイスを検出した際に同時にSNMP pollingを試みるときに使用するCommunity String
      複数定義することが可能で、上から順番に試していく
      - *When SevOne NMS discovers a device and attempts to poll SNMP data, the first string in the list is tested. If that string fails, the subsequent strings are tested, in sequence, until a string is successful. The successful community string appears on the Edit Device page for the device.*
    - 初期状態ではRead Communityに“public”が、Write Communityに“private”が登録されている
    - 本検証においては、Read Community / Write Communityに“SevOne-Test”を追加



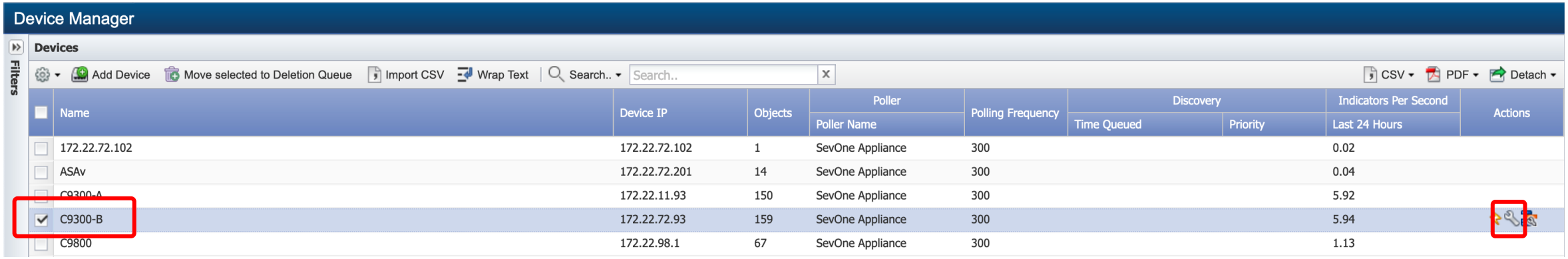
©2022 IBM Corporation

3.1.2.1. NMSの設定 (2/6)

- NMS管理下のデバイスに対する個別のSNMP設定
  - メニュー・バーより、[Devices] > [Device Manager] を選択



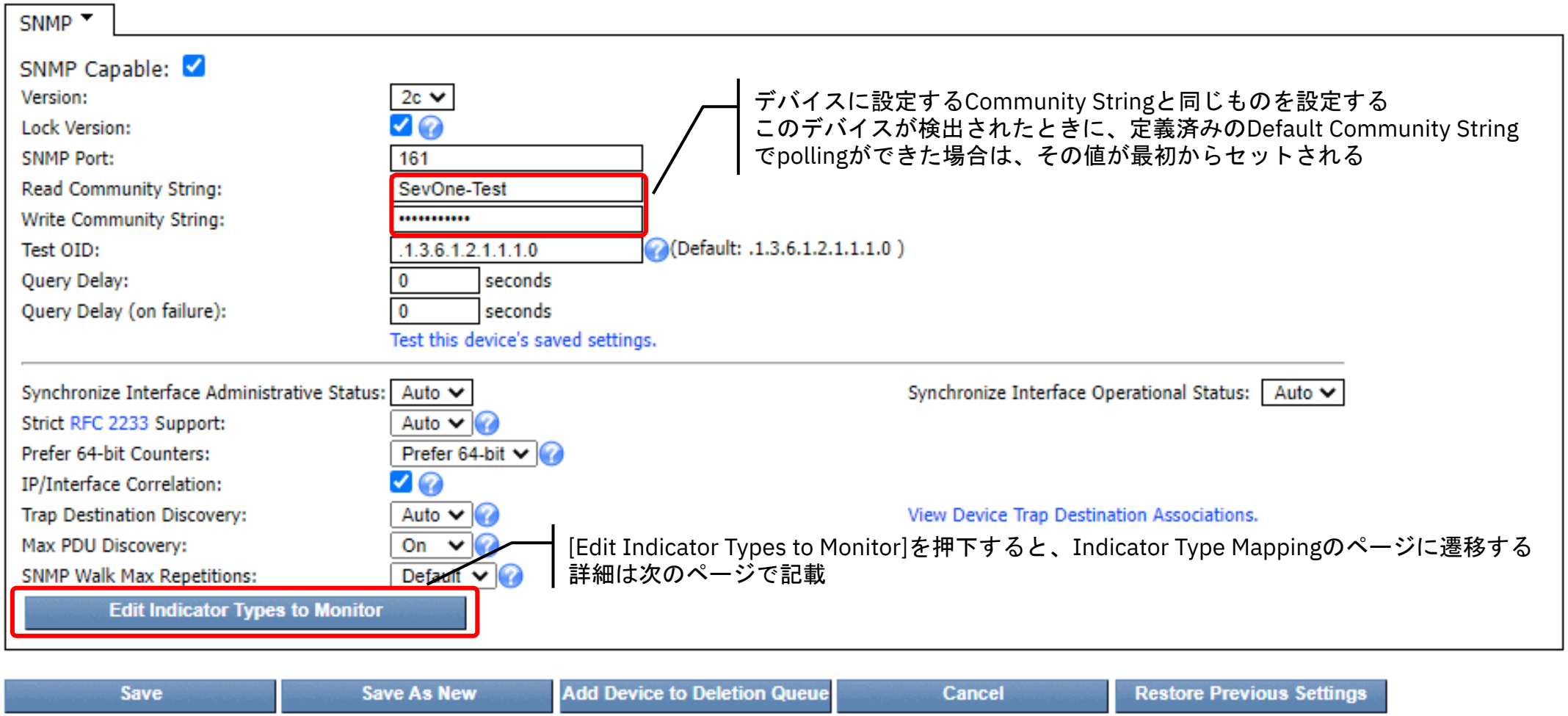
  - 対象デバイスを選択し、[Actions] 列真ん中の [Edit this device] アイコンを選択



©2022 IBM Corporation

3.1.2.1. NMSの設定 (3/6)

- NMS管理下のデバイスに対する個別のSNMP設定
  - 画面下部のPluginの箇所で [SNMP] を選択し、各種パラメーターを設定



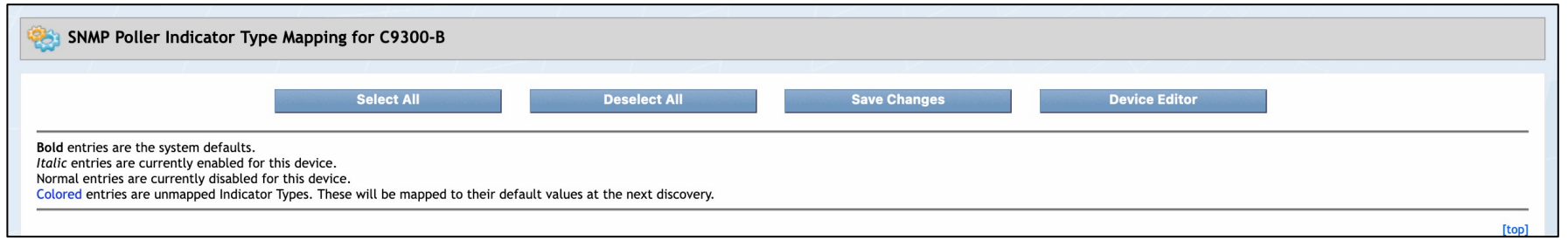
デバイスに設定するCommunity Stringと同じものを設定する
このデバイスが検出されたときに、定義済みのDefault Community String
でpollingができた場合は、その値が最初からセットされる

[Edit Indicator Types to Monitor]を押下すると、Indicator Type Mappingのページに遷移する
詳細は次のページで記載

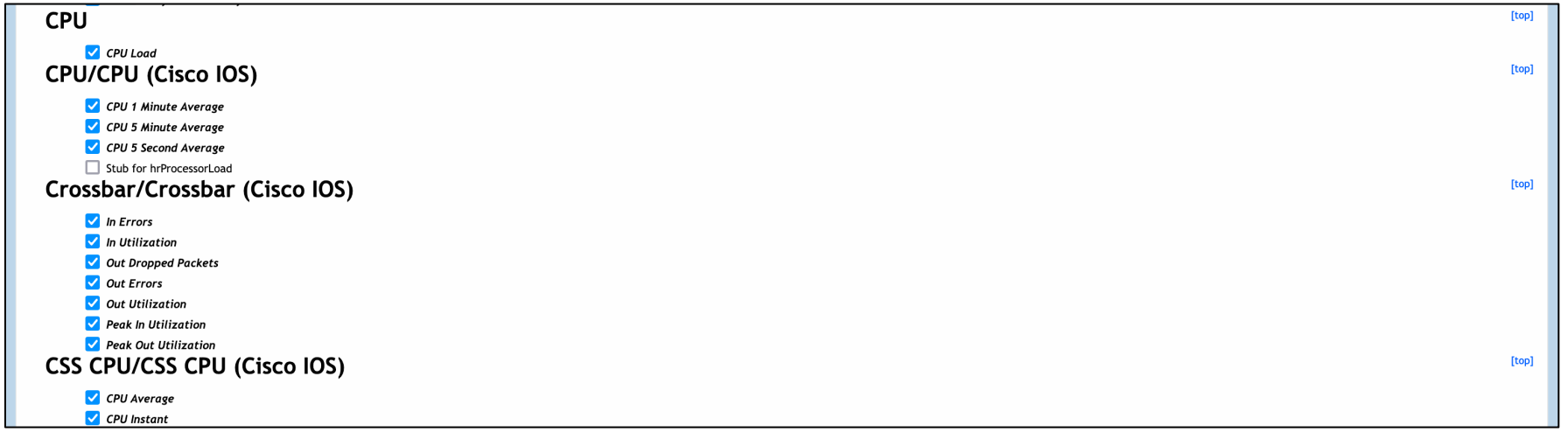
©2022 IBM Corporation

3.1.2.1. NMSの設定 (4/6)

- SNMP Polling 監視項目の設定
  - 前ページの [Edit Indicator Types to Monitor] を押下した後の画面 (SNMP Poller Indicator Type Mapping)
  - チェックが入っている項目はpolling監視対象
  - 当画面に全てのMIB/OIDが含まれるわけではなく、デバイスごとによって表示される監視項目も異なる
    表示される監視項目がどのように決まっているかは次ページを参照



⋮



©2022 IBM Corporation

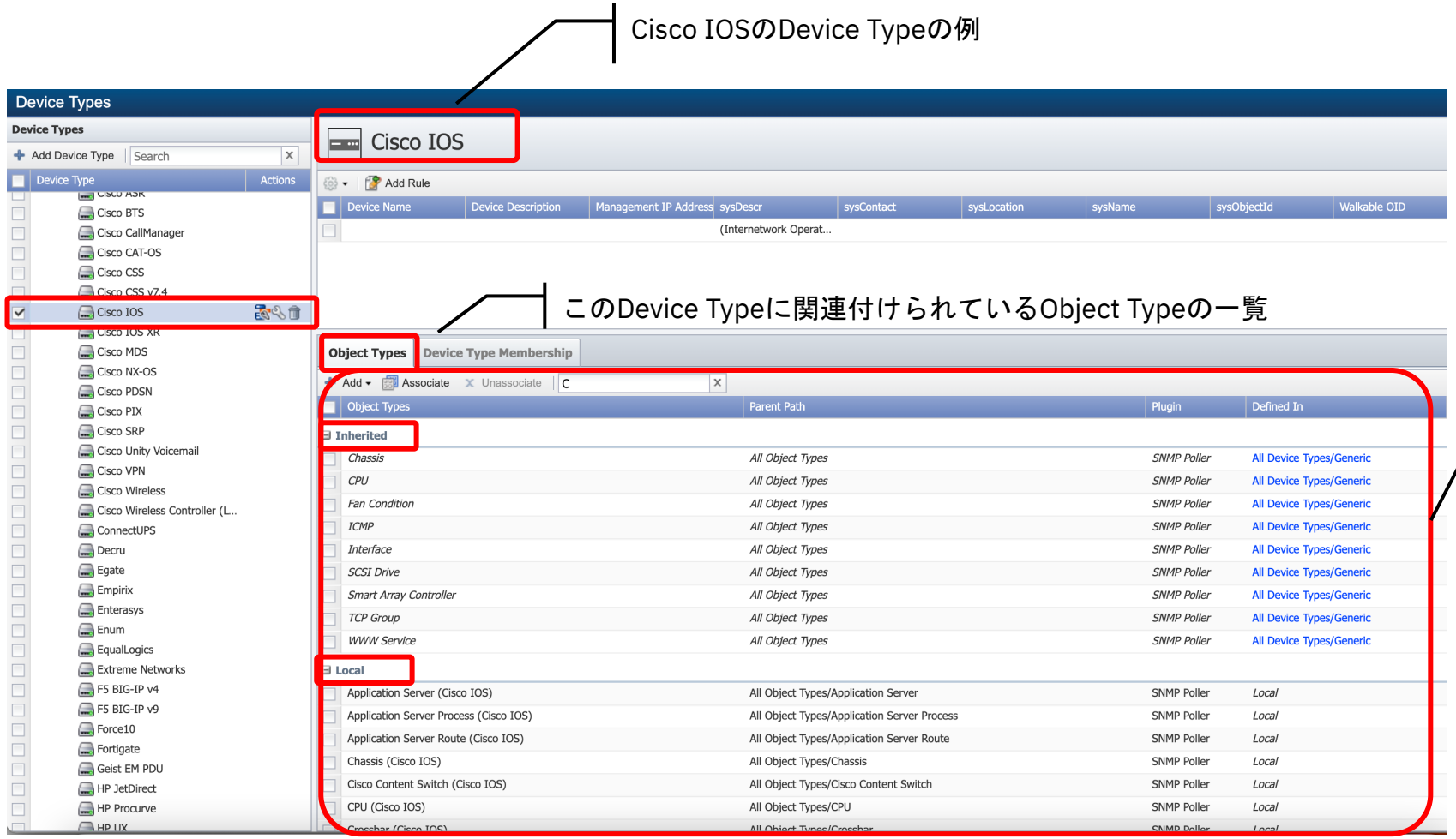
(参考) Device TypeとObject Typeについて (1/4)

- Device TypeとObject Typeについて
  - NMSには、デバイスをベンダーや機種に基づいて分類するグループ (Device Typeと呼ぶ) が定義されている
    - Device Typeは初期状態でいくつか定義されているが、新たに追加することも可能
    - 1つのデバイスは複数のDevice Typeに属することが可能
  - 各Device Typeごとに、そのDevice Typeに合わせたPolling監視項目のセット (Object Typeと呼ぶ) が関連付けられている
    - Object Typeは初期状態でいくつか定義されているが、新たにObject Typeを追加することも可能
    - 初期状態で定義されているDevice TypeにはObject Typeの関連付けも最初から定義されているが、カスタマイズ可能
- 前ページの画面 (SNMP Poller Indicator Type Mapping) には、そのデバイスが属すDevice Typeに関連づけられたObject Typeが表示されている、という関係になっている

©2022 IBM Corporation

(参考) Device TypeとObject Typeについて (2/4)

- Device Type
  - [Administration] > [Monitoring Configuration] > [Device Types]



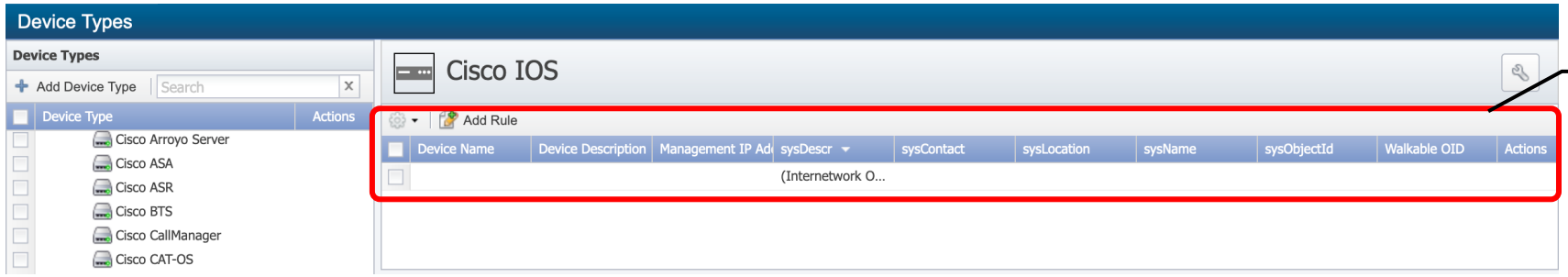
©2022 IBM Corporation

(参考) Device TypeとObject Typeについて (3/4)

■ デバイスをDevice Typeに登録する方法

– 自動での登録

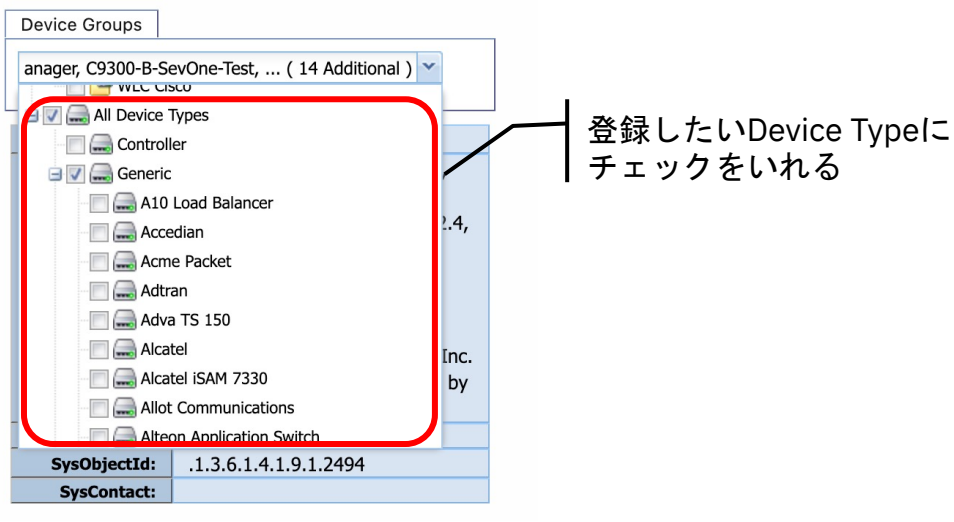
- Device TypeにAdd Ruleを定義し、ある特定の条件に一致したらそのDevice Typeに属するよう設定する



Add Ruleの条件に一致したデバイスは、
自動的にこのDevice Typeへ追加される

– 手動での登録

- [Devices] > [Device Manager] > [Edit This Device] の画面にて、Device Groupsの部分で手動登録する

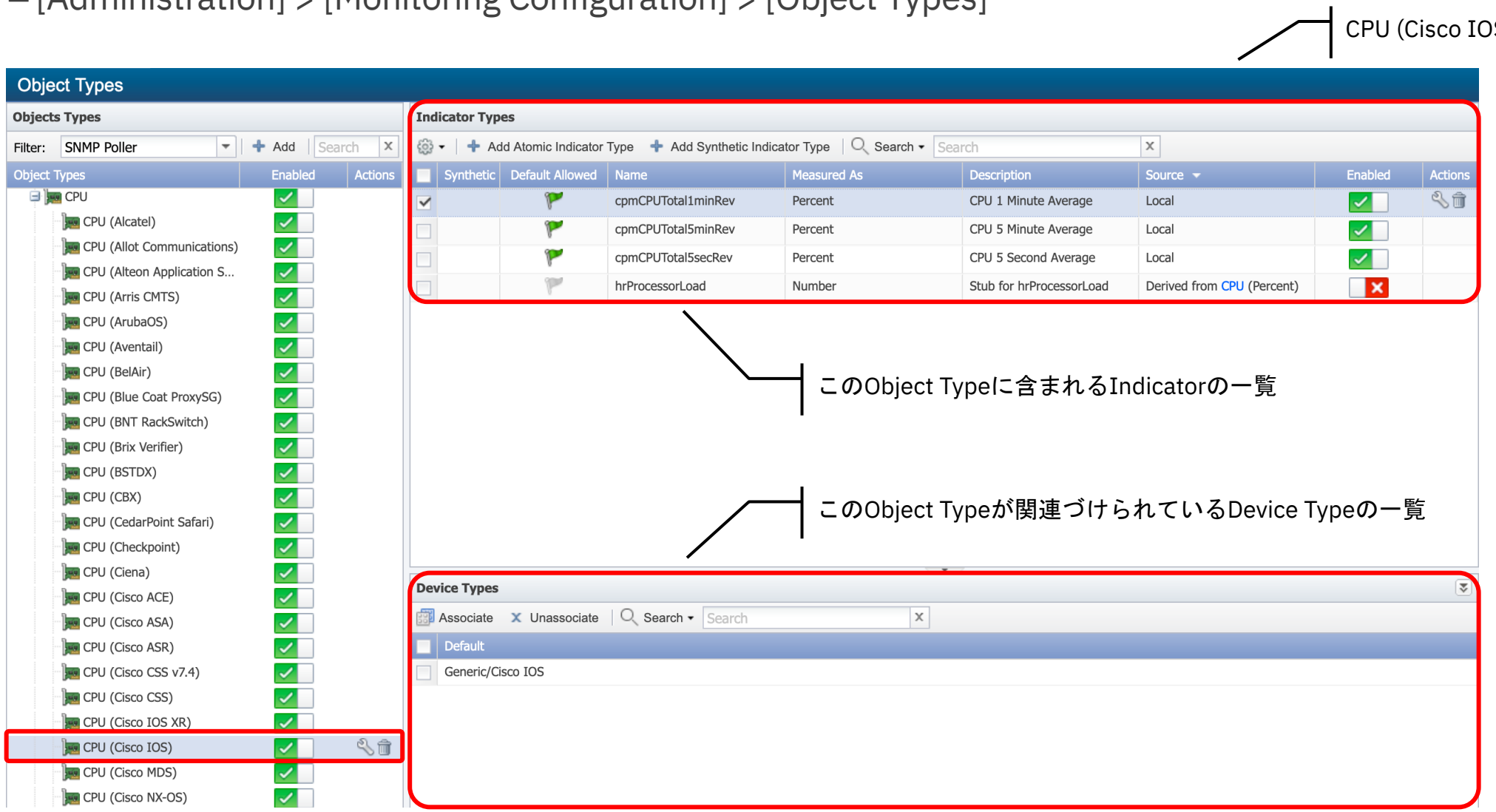


登録したいDevice Typeに
チェックをいれる

©2022 IBM Corporation

(参考) Device TypeとObject Typeについて (4/4)

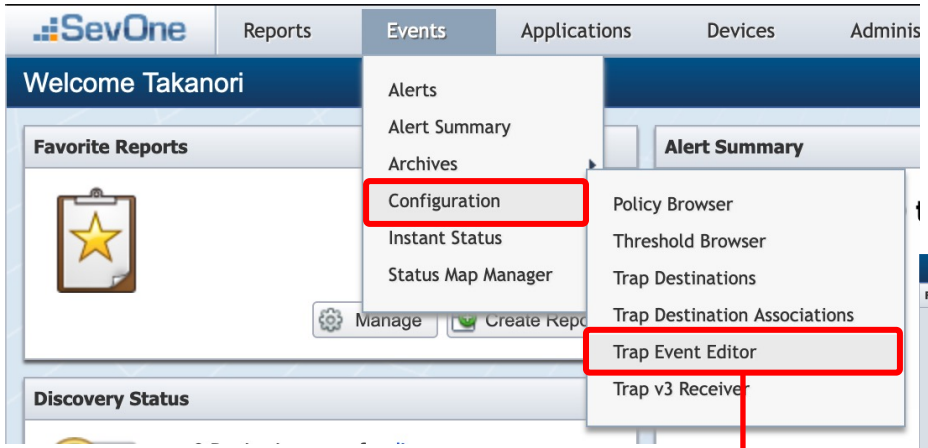
- Object Type
  - [Administration] > [Monitoring Configuration] > [Object Types]



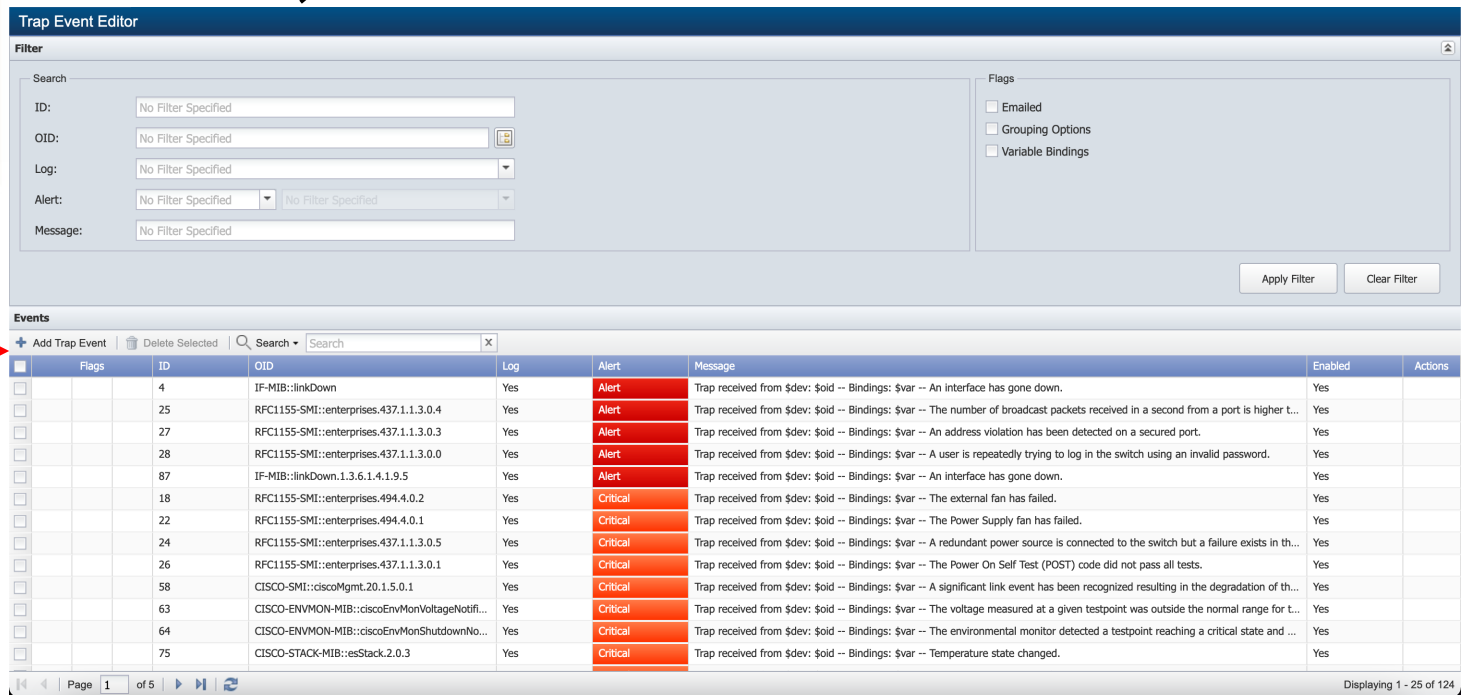
©2022 IBM Corporation

3.1.2.1. NMSの設定 (5/6)

- Trap受信時の挙動の設定
  - Trap Event Editorにて、Trap受信時の挙動を設定可能
  - [Event] > [Configuration] > [Trap Event Editor] からアクセス



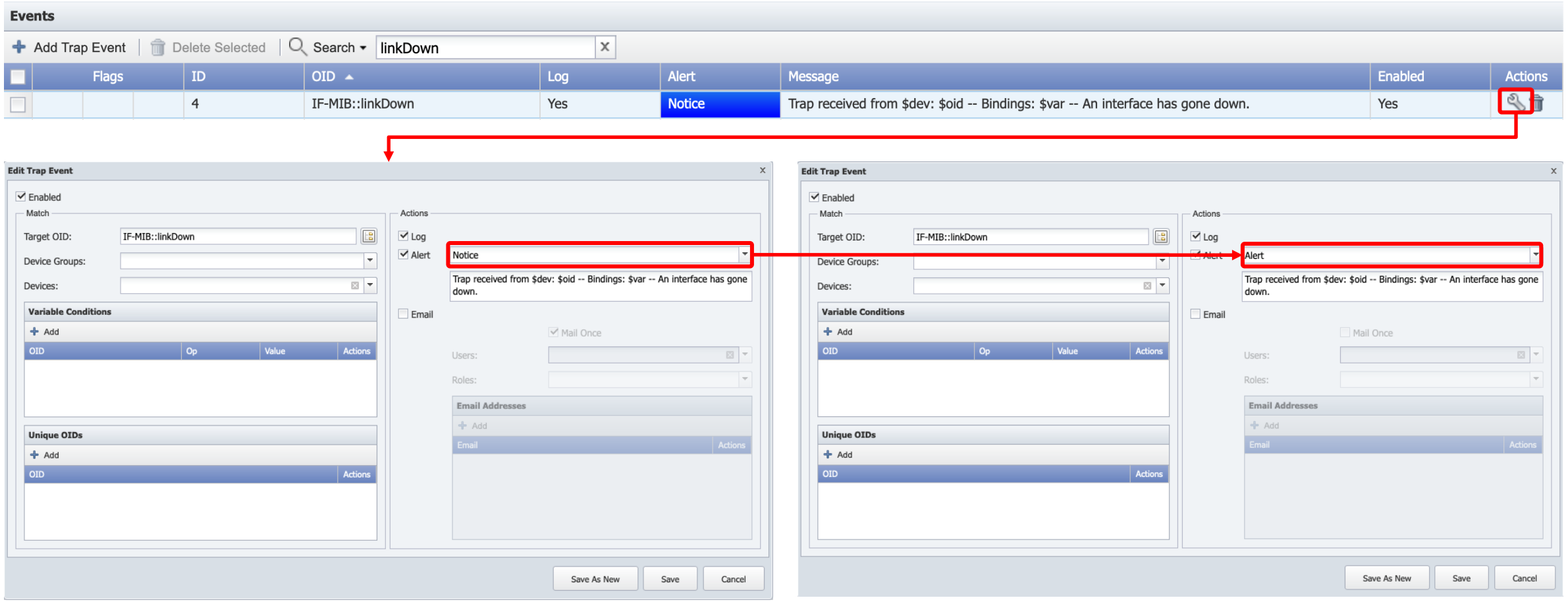
初期状態でいくつかのTrap Eventが定義されている



©2022 IBM Corporation

3.1.2.1. NMSの設定 (6/6)

- Trap受信時の挙動の設定
  - 定義済みのTrap Eventを変更するには、対象のTrap Eventを選択し、[Actions] 列の [Edit] アイコンを選択
  - 今回はIF-MIB::linkDownのTrapを受信した際のActionを次の通り変更
    - Alert のSeverityレベルを初期設定値の“Notice”から“Alert”に変更



©2022 IBM Corporation

3.1.2.2. デバイスのSNMP設定 (Ciscoデバイス)

Catalyst 9300のSample Config

```
C9300-B#show running-config | i snmp-server
snmp-server community SevOne-Test RW
snmp-server enable traps xx
snmp-server host 172.22.160.51 version 2c SevOne-Test
```

有効にするTrapを設定 (“snmp-server enable traps” コマンドで一括登録)

Catalyst 9800のSample Config

```
C9800-1# show running-config | i snmp-server
snmp-server community SevOne-Test RW
snmp-server enable traps xx
snmp-server host 172.22.160.51 version 2c SevOne-Test


# APのTrapを有効にするための追加設定
C9800-1# show running-config | i snmp-server
snmp-server enable traps wireless AP

C9800-1# show running-config | i trapflags
trapflags ap xx
```

有効にするTrapを設定 (“snmp-server enable traps” コマンドで一括登録)

APのTrapを有効化

有効にするAP関連のTrapを設定

Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Bengaluru 17.6.x
Chapter: SNMP Traps
Enabling Access Points Traps (CLI)
https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-6/config-guide/b_wl_17_6_cg/m_snmp_wireless_traps.html#Cisco_Task.dita_86e39a90-ad41-4467-a957-734bc2717b3d

©2022 IBM Corporation

3.1.2.2. デバイスのSNMP設定 (Juniperデバイス)

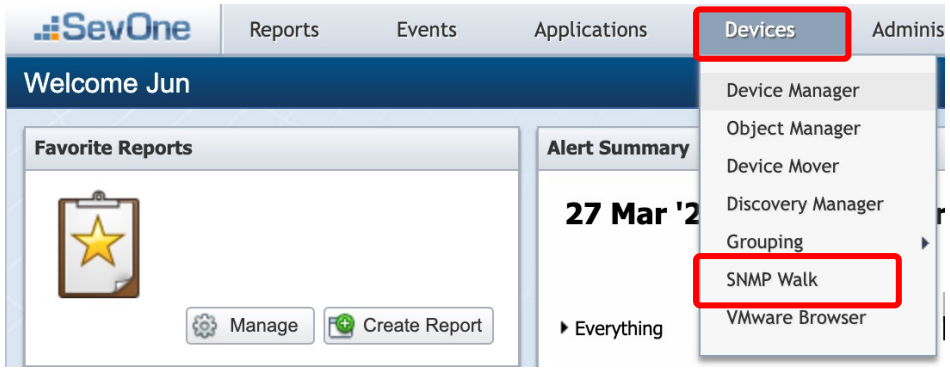
- vSRXのSample Config

```
juniper> show configuration snmp | display set
set snmp community SevOne-Test authorization read-write
set snmp community SevOne-Test clients 172.22.0.0/16
set snmp trap-group SevOne version v2
set snmp trap-group SevOne targets 172.22.160.51
```

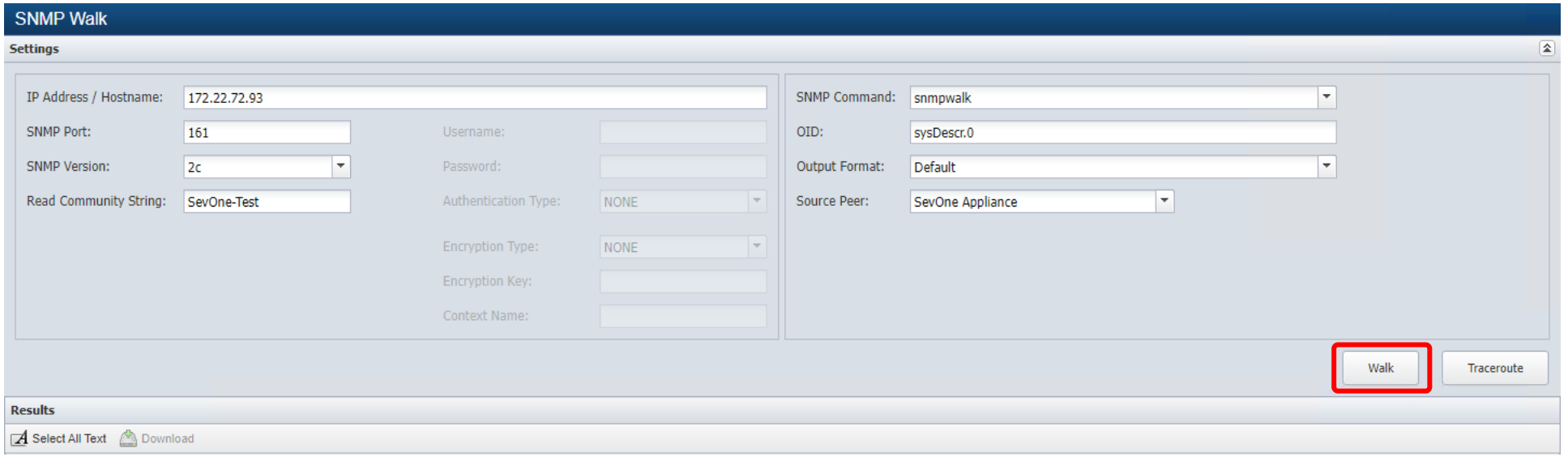

@2022 IBM Corporation

3.1.3. SNMP Walk (1/2)

- [Devices] > [SNMP Walk] を選択



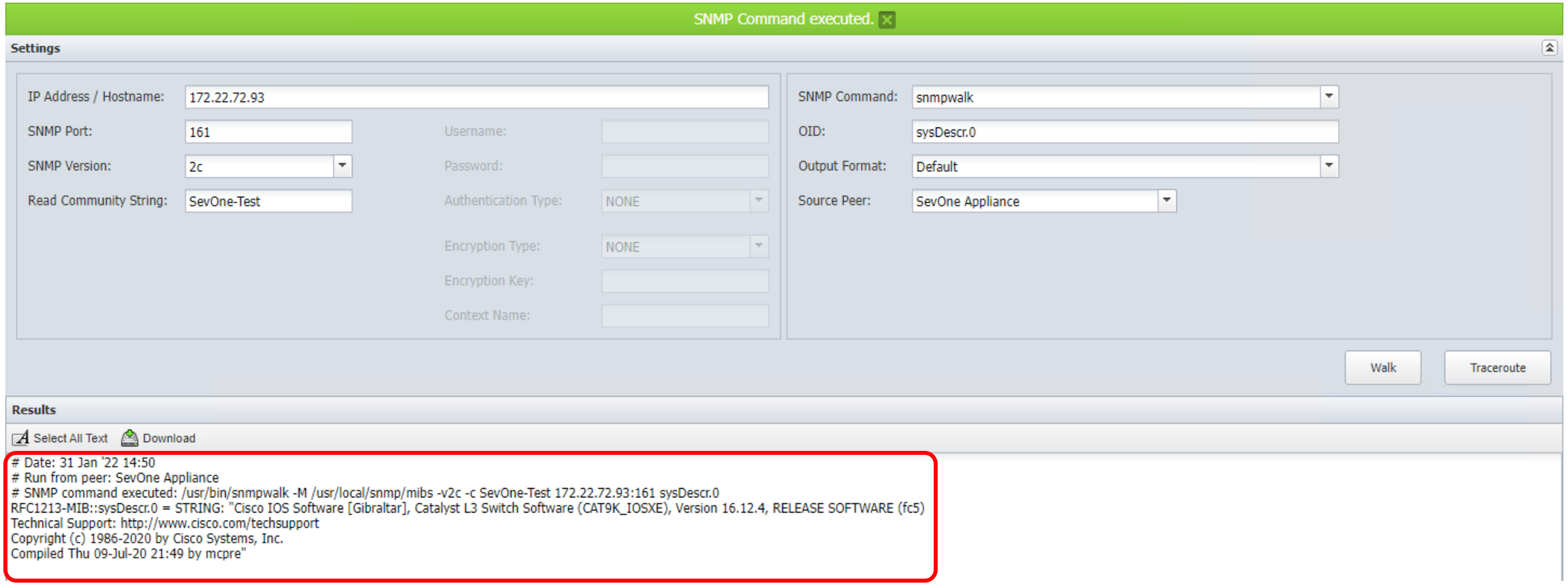
- 対象アドレスやCommunity-Stringなど各パラメータを入力し、Walkを押下する



©2022 IBM Corporation

3.1.3. SNMP Walk (2/2)

■ 入力したパラメーターでNMSからSNMP Walkが実施できれば、Resultに結果が表示される



©2022 IBM Corporation

3.1.3. SNMP Trap受信 (1/4)

■ Catalyst 9300での疑似障害

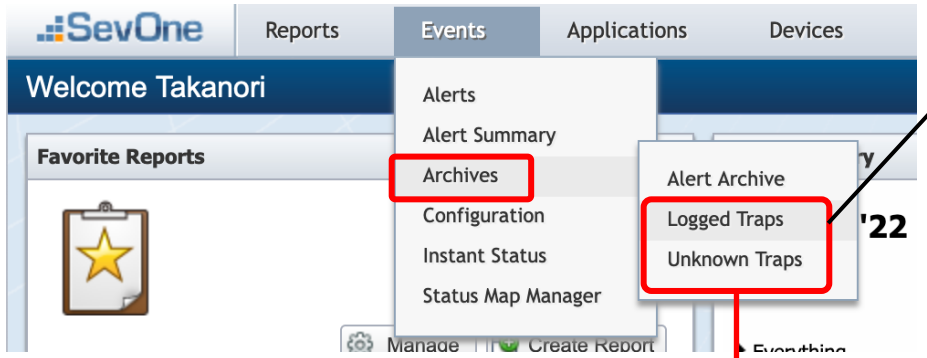
```
C2960-R12#show cdp neighbors
<snip>
C9300-B.iselab.local
            Gig 1/0/17      124          R S I  C9300-48U Gig 1/0/13
<snip>
C2960-R12#configure t
C2960-R12(config)#int g 1/0/17
C2960-R12(config-if)#shutdown
```

C9300-Bが直結しているL2スイッチ(C2960-R12) にて、
接続Interfaceをshutdownする

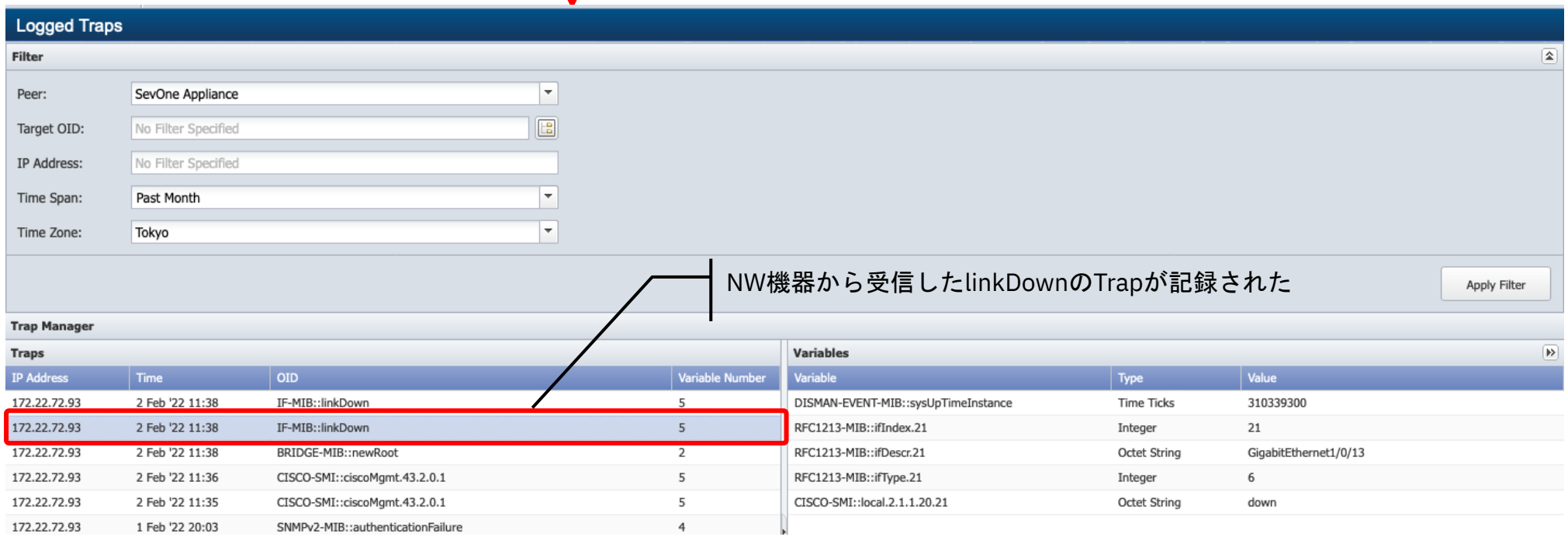
©2022 IBM Corporation

3.1.3. SNMP Trap受信 (2/4)

- Trap受信ログの確認
  - [Event] > [Archives] > [Logged Traps] または [Unknown Traps] を選択



Logged Traps : Trap Eventが定義されているTrapが記録される
Unknown Traps : Trap Eventが定義されていないTrapが記録される

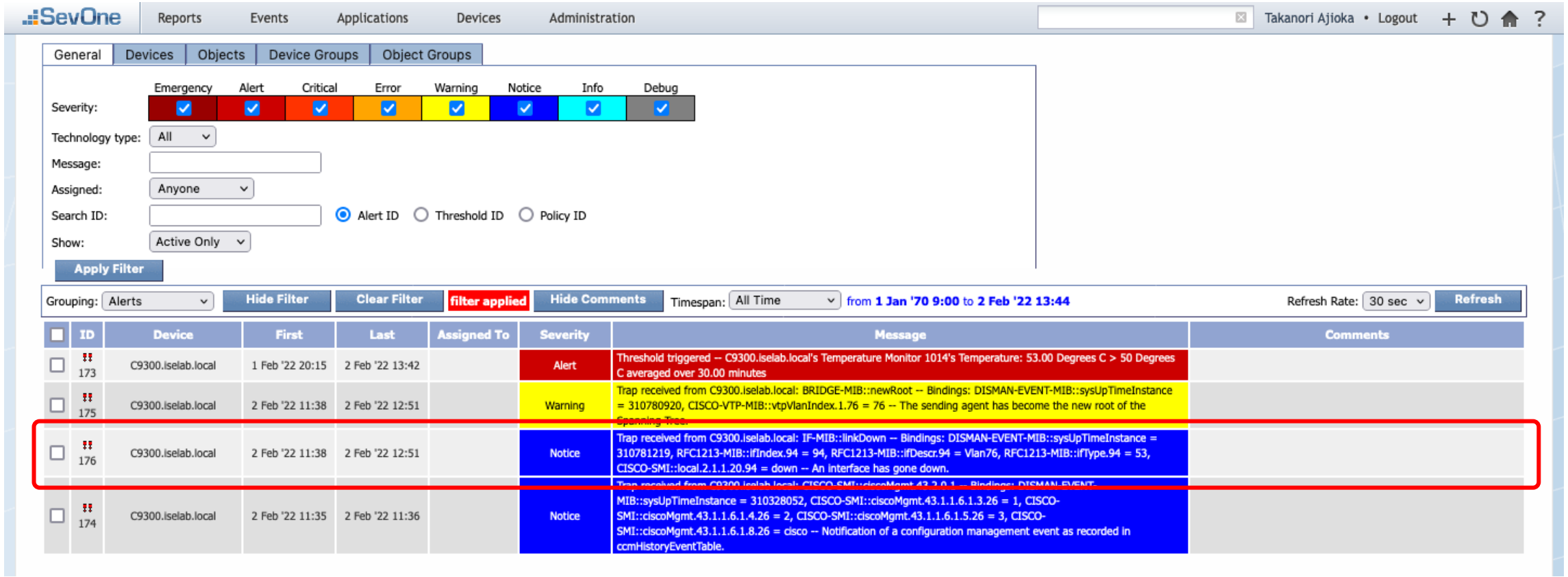


NW機器から受信したlinkDownのTrapが記録された

©2022 IBM Corporation

3.1.3. SNMP Trap受信 (3/4)

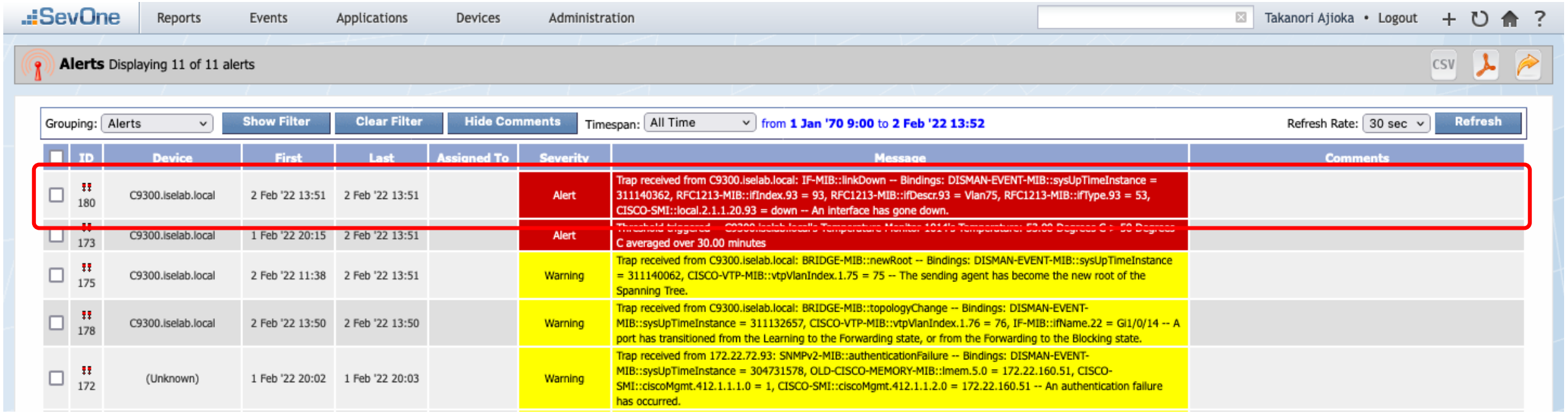
- Trap Eventの動作確認
  - [Event] > [Alerts] にてNMSが発報したAlertを表示
  - こちらのTrap Eventの変更前、linkDownのTrapに対するAlertは、Severity LevelがNoticeであった



©2022 IBM Corporation

3.1.3. SNMP Trap受信 (4/4)

- Trap Eventの動作確認
  - こちらのTrap Eventの変更後、linkDownのTrapに対するAlertは、Severity LevelがAlertになった
    - 補足：
      すでにTrapが発報された状態でTrap EventのSeverityを変更したところ、新しく発報されたTrapも変更前のSeverityで記録された (別のIDのAlertとして発報されずLastの日時が更新されただけであった)
      一度、AcknowledgeをしてAlertを消した後に、新しいIDで発報されたTrapは、変更後のSeverityで記録された。



ID	Device	First	Last	Assigned To	Severity	Message	Comments
180	C9300.iselab.local	2 Feb '22 13:51	2 Feb '22 13:51		Alert	Trap received from C9300.iselab.local: IF-MIB::linkDown -- Bindings: DISMAN-EVENT-MIB::sysUpTimeInstance = 311140362, RFC1213-MIB::ifIndex.93 = 93, RFC1213-MIB::ifDescr.93 = Vlan75, RFC1213-MIB::ifType.93 = 53, CISCO-SMI::local.2.1.1.20.93 = down -- An interface has gone down.	
173	C9300.iselab.local	1 Feb '22 20:15	2 Feb '22 13:51		Alert	[illegible] C averaged over 30.00 minutes	
175	C9300.iselab.local	2 Feb '22 11:38	2 Feb '22 13:51		Warning	Trap received from C9300.iselab.local: BRIDGE-MIB::newRoot -- Bindings: DISMAN-EVENT-MIB::sysUpTimeInstance = 311140062, CISCO-VTP-MIB::vtpVlanIndex.1.75 = 75 -- The sending agent has become the new root of the Spanning Tree.	
178	C9300.iselab.local	2 Feb '22 13:50	2 Feb '22 13:50		Warning	Trap received from C9300.iselab.local: BRIDGE-MIB::topologyChange -- Bindings: DISMAN-EVENT-MIB::sysUpTimeInstance = 311132657, CISCO-VTP-MIB::vtpVlanIndex.1.76 = 76, IF-MIB::ifName.22 = Gi1/0/14 -- A port has transitioned from the Learning to the Forwarding state, or from the Forwarding to the Blocking state.	
172	(Unknown)	1 Feb '22 20:02	1 Feb '22 20:03		Warning	Trap received from 172.22.72.93: SNMPv2-MIB::authenticationFailure -- Bindings: DISMAN-EVENT-MIB::sysUpTimeInstance = 304731578, OLD-CISCO-MEMORY-MIB::lmem.5.0 = 172.22.160.51, CISCO-SMI::ciscoMgmt.412.1.1.1.0 = 1, CISCO-SMI::ciscoMgmt.412.1.1.2.0 = 172.22.160.51 -- An authentication failure has occurred.	

©2022 IBM Corporation

3.2. IP SLA

IP SLA概要

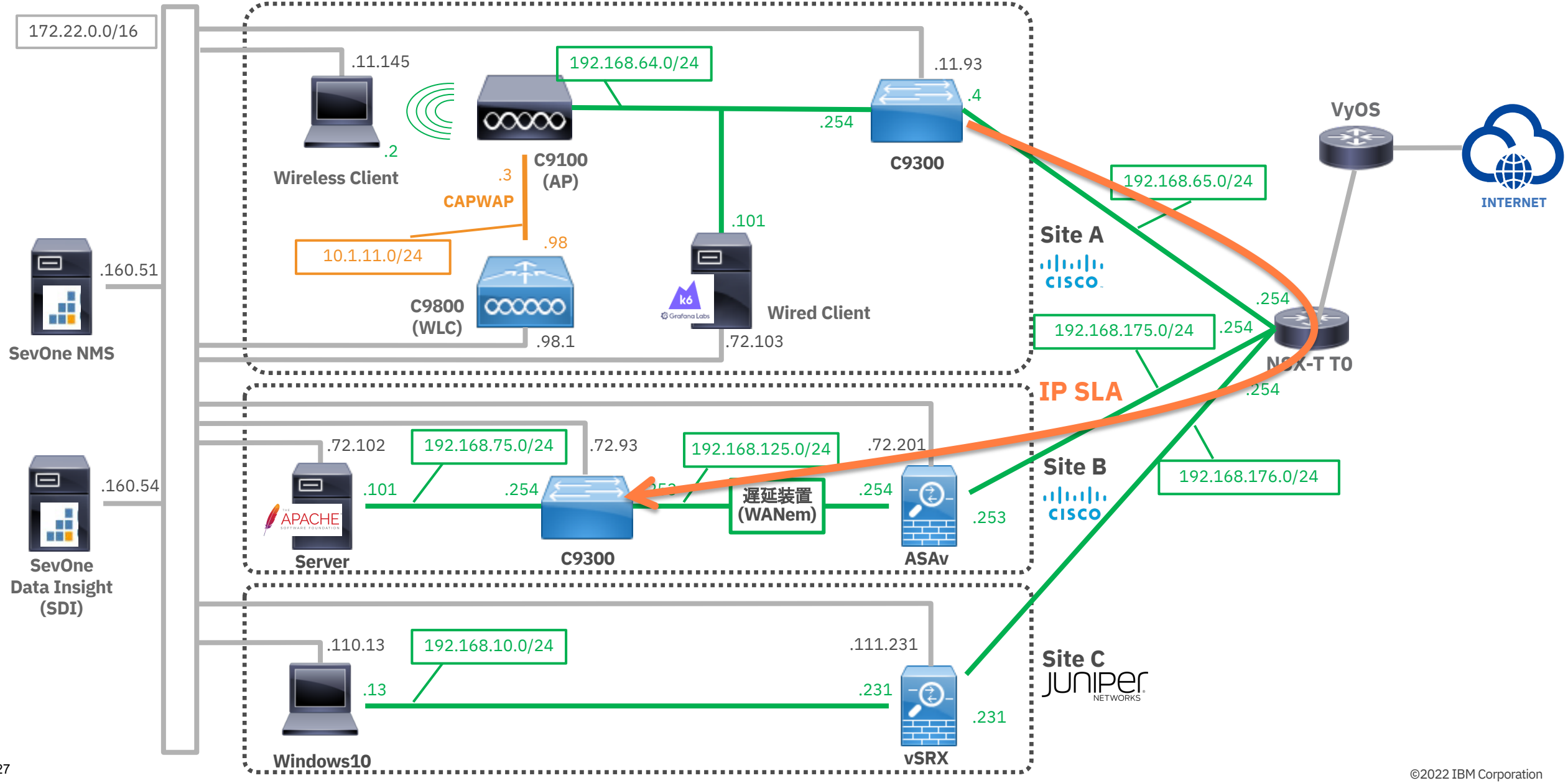
- IP SLAはCisco社が開発したネットワークのサービスレベルを測定するための技術
  - Cisco IOSを搭載したデバイスから測定用のテストパケットを送信し、到達可否や遅延、ジッタ、RTT、パケットロスなどを測定可能
- SevOne NMSはCiscoデバイスが収集したIP SLA情報をSNMPで取得する

検証内容

- Ciscoスイッチを使用してIP SLAの設定をし、遅延装置で遅延やジッタを発生させてSevOneで観測する

©2022 IBM Corporation

3.2.1. 検証構成



©2022 IBM Corporation

3.2.2. 設定

■ 設定概要

1. IP SLA Monitoring有効化
2. IP SLA設定

– 以下のいずれかの方法でIP SLAの設定が可能

(1) Cisco機器側でコマンドラインにてIP SLAを設定

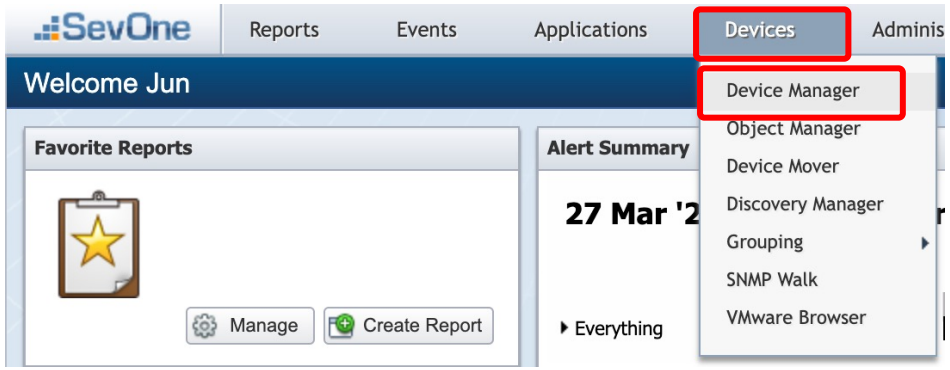
(2) SevOne NMSでIP SLAの設定を実施し、SNMPでCisco機器へ自動反映

• 簡易的な設定のみ可能で細かいパラメーターの設定は不可

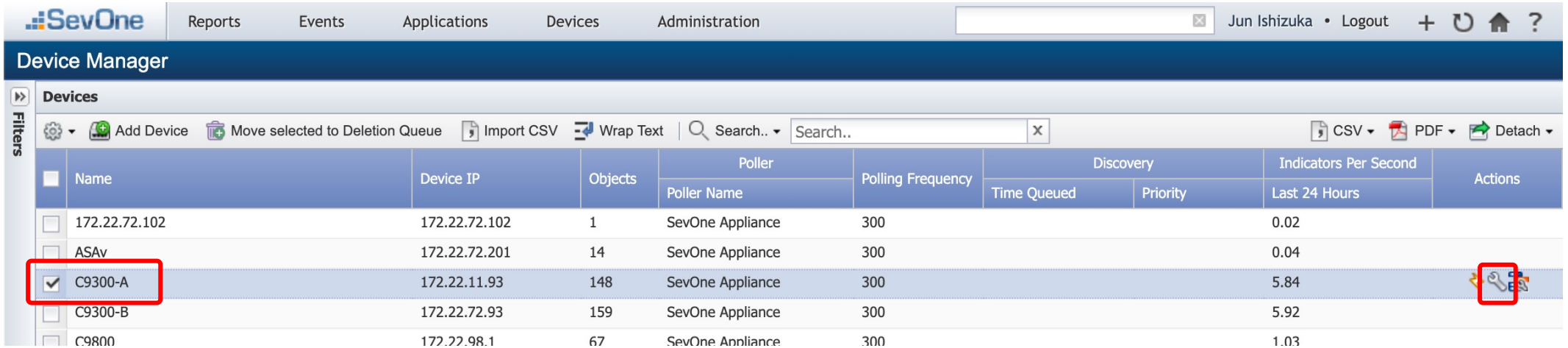
©2022 IBM Corporation

3.2.2.1. IP SLA Monitoring 有効化 (1/2)

- 管理デバイスのIP SLA Monitoring有効化
  - メニュー・バーより、[Devices] > [Device Manager] を選択



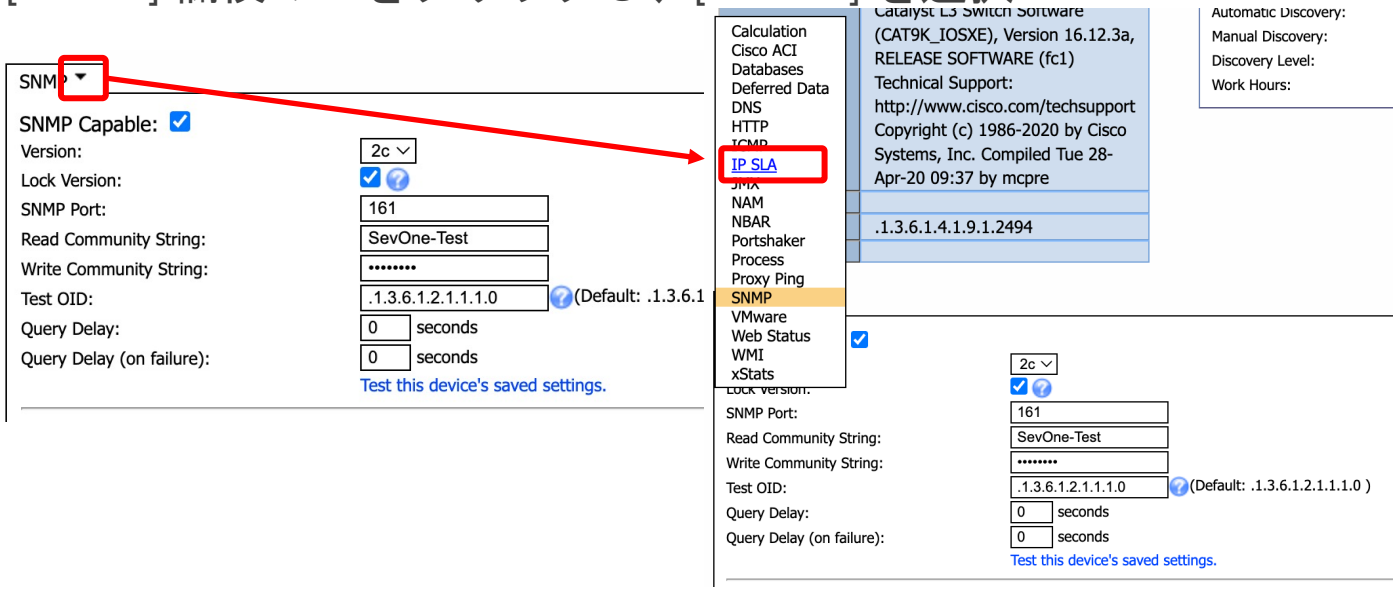
  - 対象デバイスを選択し、[Actions] 列真ん中の [Edit this device] アイコンを選択



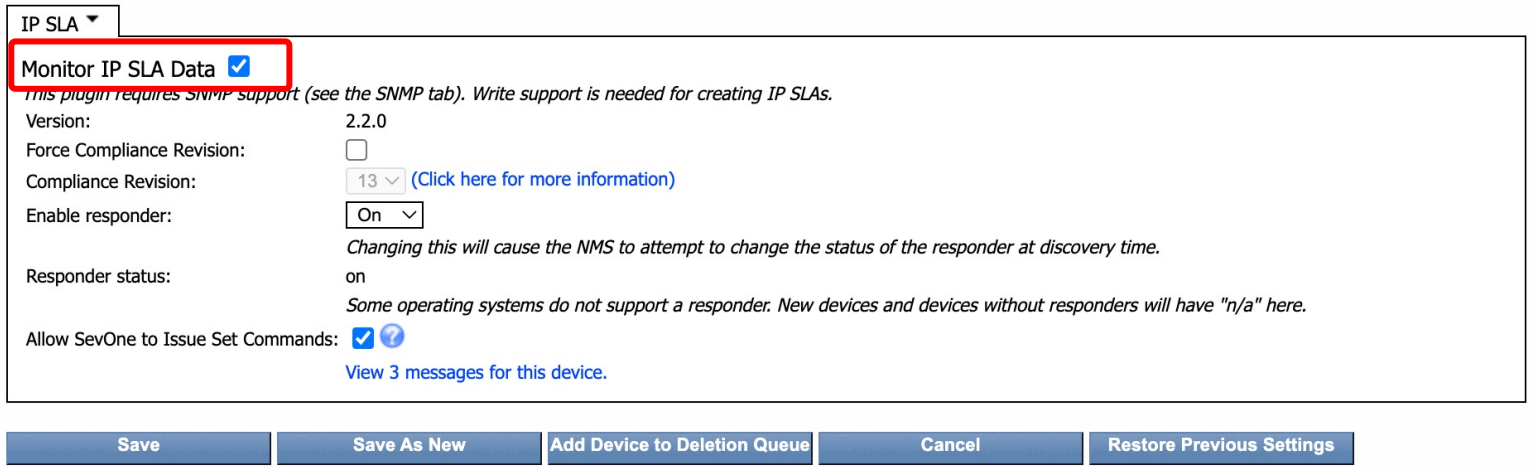
©2022 IBM Corporation

3.2.2.1. IP SLA Monitoring 有効化 (2/2)

– [SNMP] 欄横の▼をクリックし、[IP SLA] を選択



– [Monitor IP SLA Data] にチェックが付いていることを確認



©2022 IBM Corporation

3.2.2.2. IP SLA設定 (1) (1/2)

- Cisco機器のコマンドラインでIP SLAを設定
  - 例：icmp-jitter設定

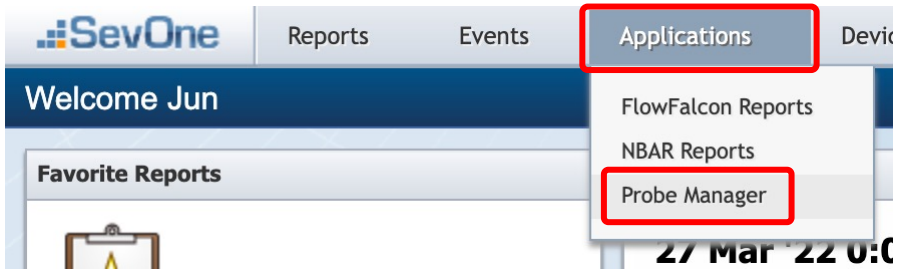
```
C9300-A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
C9300-A(config)#ip sla 1
C9300-A(config-ip-sla)#icmp-jitter 192.168.125.253 source-ip 192.168.65.4
C9300-A(config-ip-sla-icmpjitter)#threshold 100
C9300-A(config-ip-sla-icmpjitter)#timeout 1000
C9300-A(config-ip-sla-icmpjitter)#frequency 5
C9300-A(config-ip-sla-icmpjitter)#exit
C9300-A(config)#ip sla schedule 1 life forever start-time now
C9300-A(config)#end
```

```
C9300-A#show ip sla configuration 1
IP SLAs Infrastructure Engine-III
Entry number: 1
Owner:
Tag:
Operation timeout (milliseconds): 1000
Type of operation to perform: icmp-jitter
Target address/Source address: 192.168.125.253/192.168.65.4
Packet Interval (milliseconds)/Number of packets: 20/10
Type Of Service parameter: 0x0
Vrf Name:
Schedule:
  Operation frequency (seconds): 5  (not considered if randomly scheduled)
  Next Scheduled Start Time: Start Time already passed
  Group Scheduled : FALSE
  Randomly Scheduled : FALSE
  Life (seconds): Forever
  Entry Ageout (seconds): never
  Recurring (Starting Everyday): FALSE
  Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 100
Distribution Statistics:
  Number of statistic hours kept: 2
  Number of statistic distribution buckets kept: 1
  Statistic distribution interval (milliseconds): 20
Enhanced History:
Percentile:
```

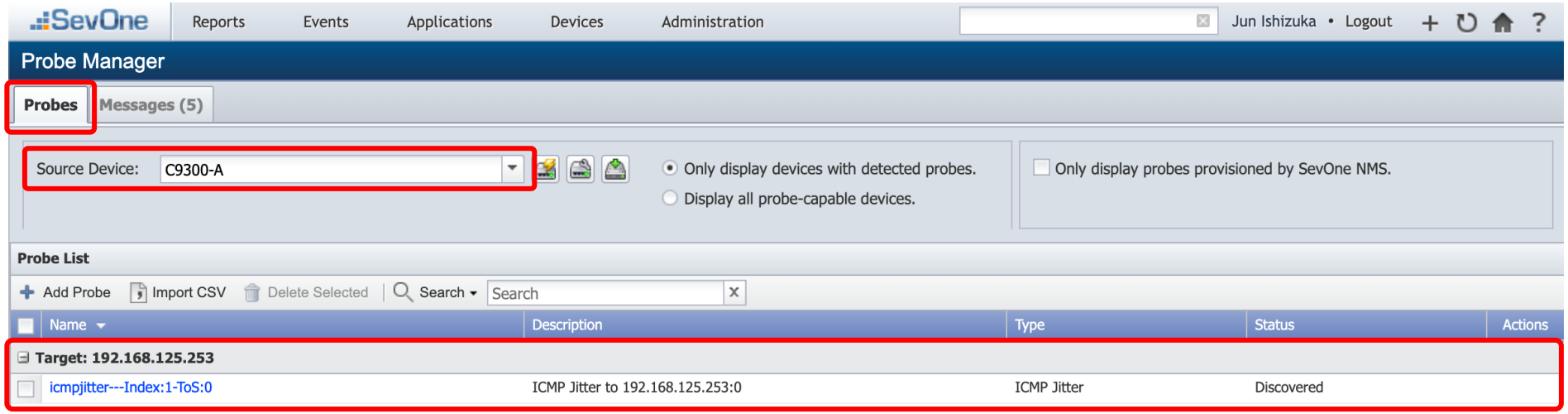

©2022 IBM Corporation

3.2.2.2. IP SLA設定 (1) (2/2)

- しばらくするとCisco機器にて設定した内容がSevOne側で認識される
  - メニュー・バーより、[Applications] > [Probe Manager] を選択



  - [Probes] タブの [Source Device] で対象デバイスを選択すると、Cisco機器のIP SLA設定が表示される

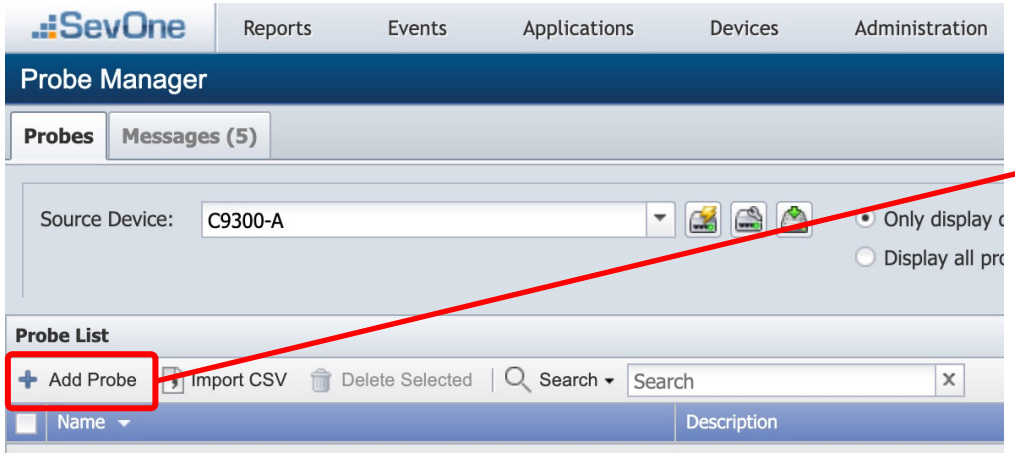


©2022 IBM Corporation

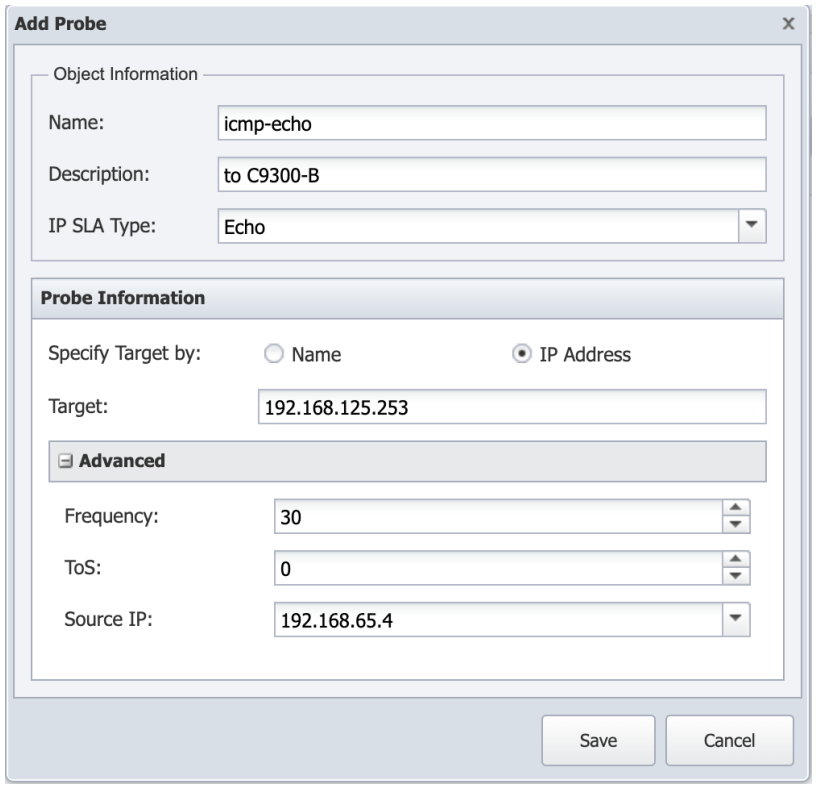
3.2.2.2. IP SLA設定 (2) (1/3)

- SevOne NMSにてIP SLAを作成し、Cisco機器に自動反映
  - 前提としてSNMPによる書き込み権限が必要

  - [Probes] タブの [Source Device] で対象デバイスを選択し、[Add Probe] ボタンを押下
  - IP SLAの設定を作成し、[Save] ボタンを押下



例：icmp-echo設定

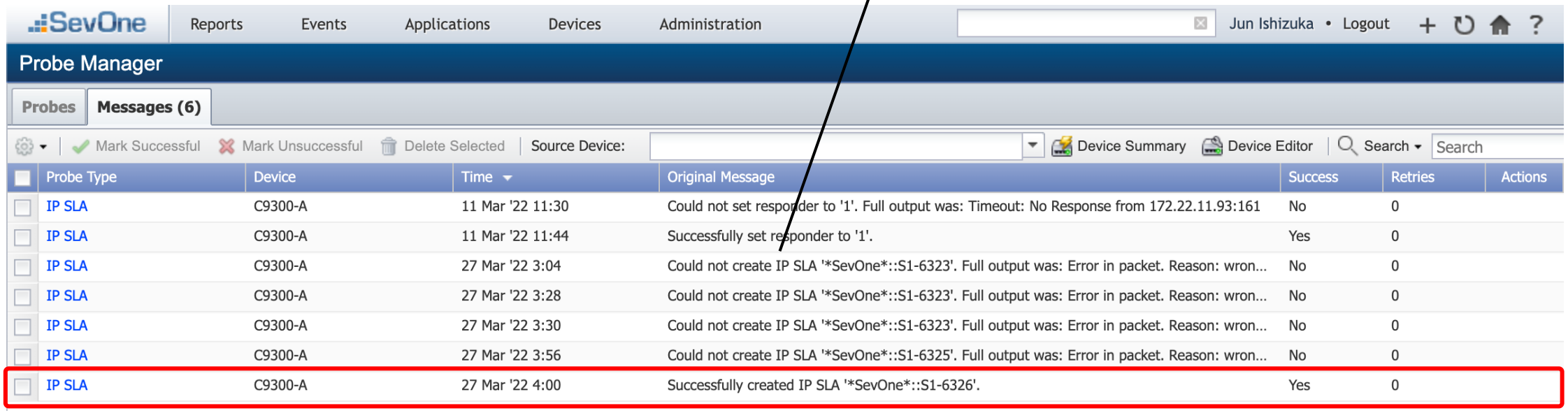


©2022 IBM Corporation

3.2.2.2. IP SLA設定 (2) (2/3)

– [Save] ボタンを押下するとCisco機器にSNMPで設定が自動反映される
  • [Messages] タブにて [Success] 列が「Yes」となっていれば設定投入が成功

設定パラメーターの値に問題がある場合Cisco機器への設定反映が失敗することがある



Probe Type	Device	Time	Original Message	Success	Retries	Actions
IP SLA	C9300-A	11 Mar '22 11:30	Could not set responder to '1'. Full output was: Timeout: No Response from 172.22.11.93:161	No	0	
IP SLA	C9300-A	11 Mar '22 11:44	Successfully set responder to '1'.	Yes	0	
IP SLA	C9300-A	27 Mar '22 3:04	Could not create IP SLA '*SevOne*::S1-6323'. Full output was: Error in packet. Reason: wron...	No	0	
IP SLA	C9300-A	27 Mar '22 3:28	Could not create IP SLA '*SevOne*::S1-6323'. Full output was: Error in packet. Reason: wron...	No	0	
IP SLA	C9300-A	27 Mar '22 3:30	Could not create IP SLA '*SevOne*::S1-6323'. Full output was: Error in packet. Reason: wron...	No	0	
IP SLA	C9300-A	27 Mar '22 3:56	Could not create IP SLA '*SevOne*::S1-6325'. Full output was: Error in packet. Reason: wron...	No	0	
IP SLA	C9300-A	27 Mar '22 4:00	Successfully created IP SLA '*SevOne*::S1-6326'.	Yes	0	

©2022 IBM Corporation

3.2.2.2. IP SLA設定 (2) (3/3)

- Cisco機器のコマンドにて設定が反映されたことを確認可能

```
C9300-A#show ip sla configuration
(中略)
Entry number: 2
Owner: *SevOne*
Tag: S1-6326
Operation timeout (milliseconds): 20000
Type of operation to perform: icmp-echo
Target address/Source address: 192.168.125.253/192.168.65.4
Type Of Service parameter: 0x0
Request size (ARR data portion): 28
Data pattern: 0xABCDABCD
Verify data: No
Vrf Name:
Schedule:
   Operation frequency (seconds): 30  (not considered if randomly scheduled)
   Next Scheduled Start Time: Start Time already passed
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): Forever
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): Active
Threshold (milliseconds): 5000
Distribution Statistics:
   Number of statistic hours kept: 2
   Number of statistic distribution buckets kept: 1
   Statistic distribution interval (milliseconds): 20
Enhanced History:
History Statistics:
   Number of history Lives kept: 0
   Number of history Buckets kept: 15
   History Filter Type: None
```


©2022 IBM Corporation

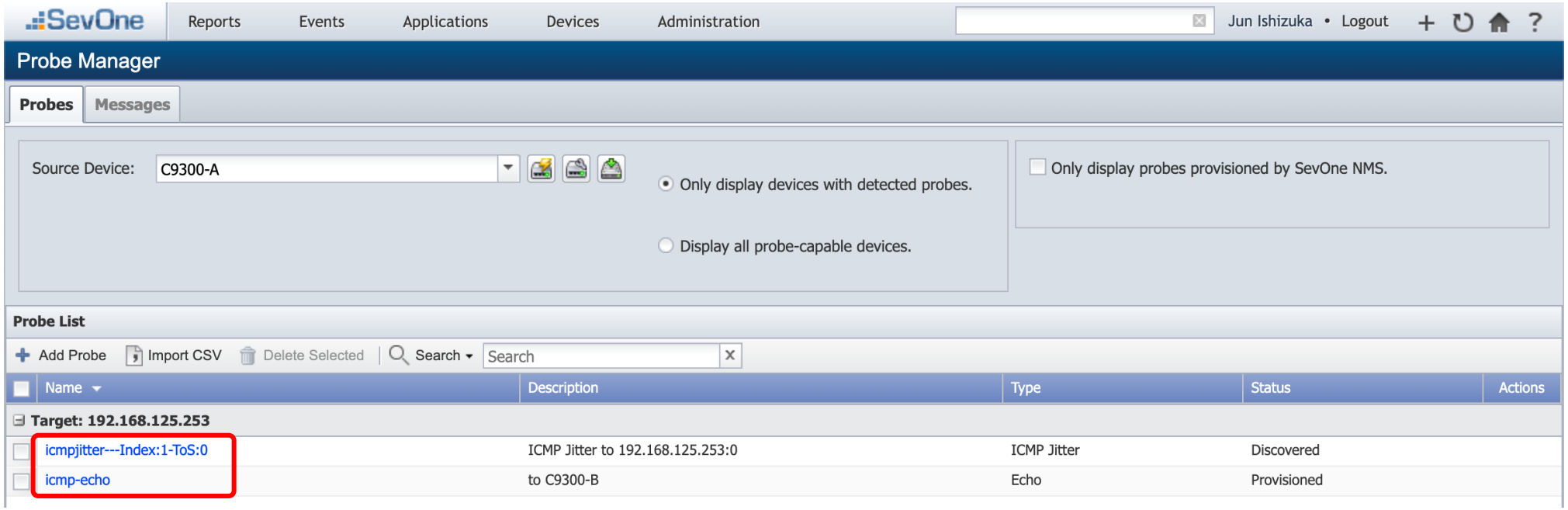
(参考) SevOne NMSでサポートされるIP SLA

- 以下のIP SLAタイプがサポートされる
  - DHCP
  - DLSw
  - DNS
  - Echo
  - Ethernet Jitter
  - Ethernet Ping
  - FTP
  - HTTP
  - ICMP Jitter
  - RTP
  - TCP Connect
  - UDP Echo
  - UDP Jitter
  - Video
  - VoIP

©2022 IBM Corporation

3.2.3. IP SLAモニタリング (1/4)

- SevOne NMS
  - メニュー・バーの [Applications] > [Probe Manager] より、該当のProbeのリンクをクリックすることでレポートを確認可能

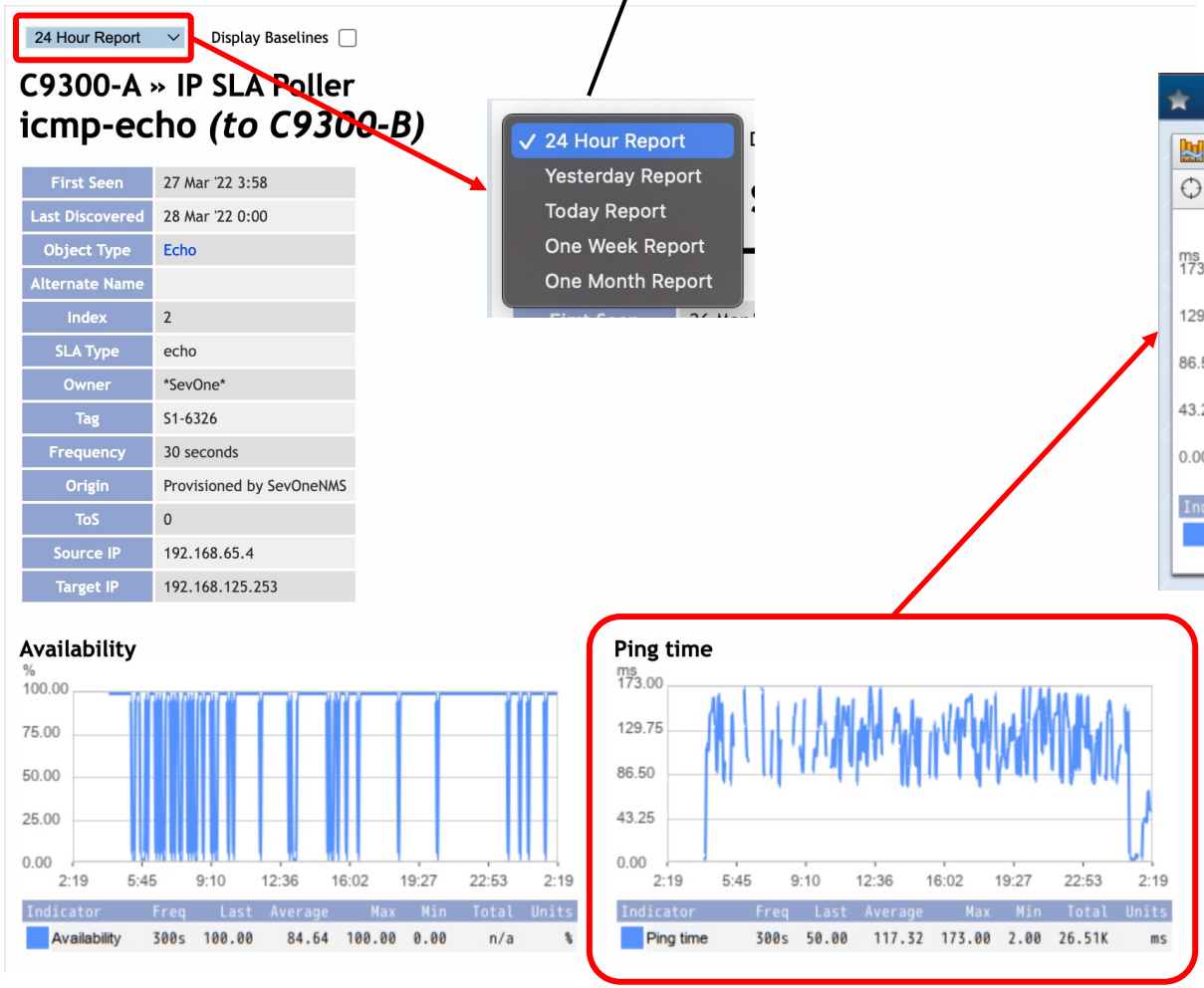


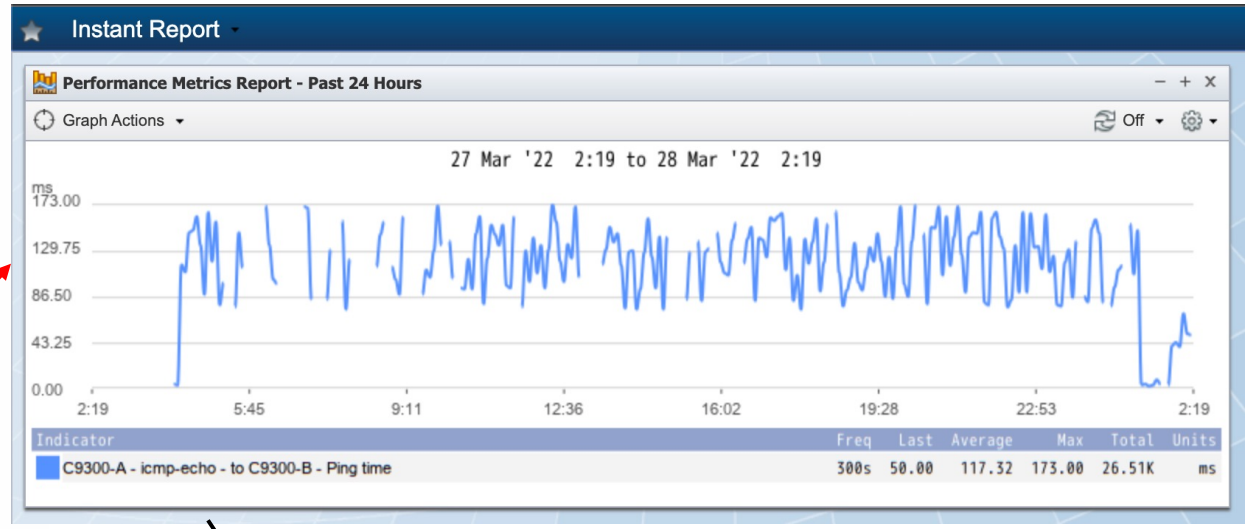
©2022 IBM Corporation

3.2.3. IP SLAモニタリング (2/4)

- SevOne NMS
  - icmp-echo

表示するレポートの期間を選択可能



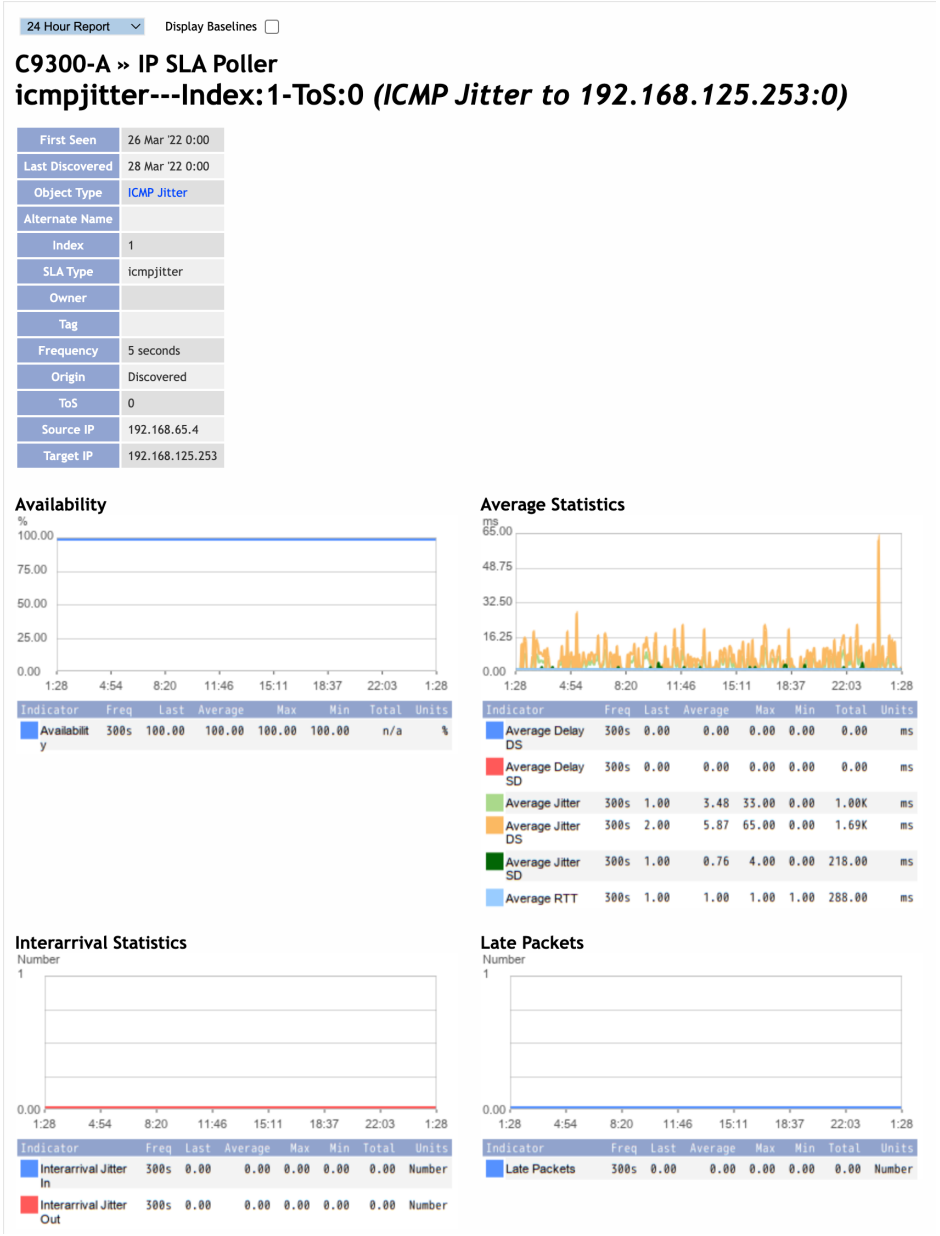


グラフをクリックすると、Instant Report画面が表示される。
Instant Reportでは、タイムスパンの柔軟な変更や、グラフの編集、CSV形式のエクスポートなどが可能。

©2022 IBM Corporation

3.2.3. IP SLAモニタリング (3/4)

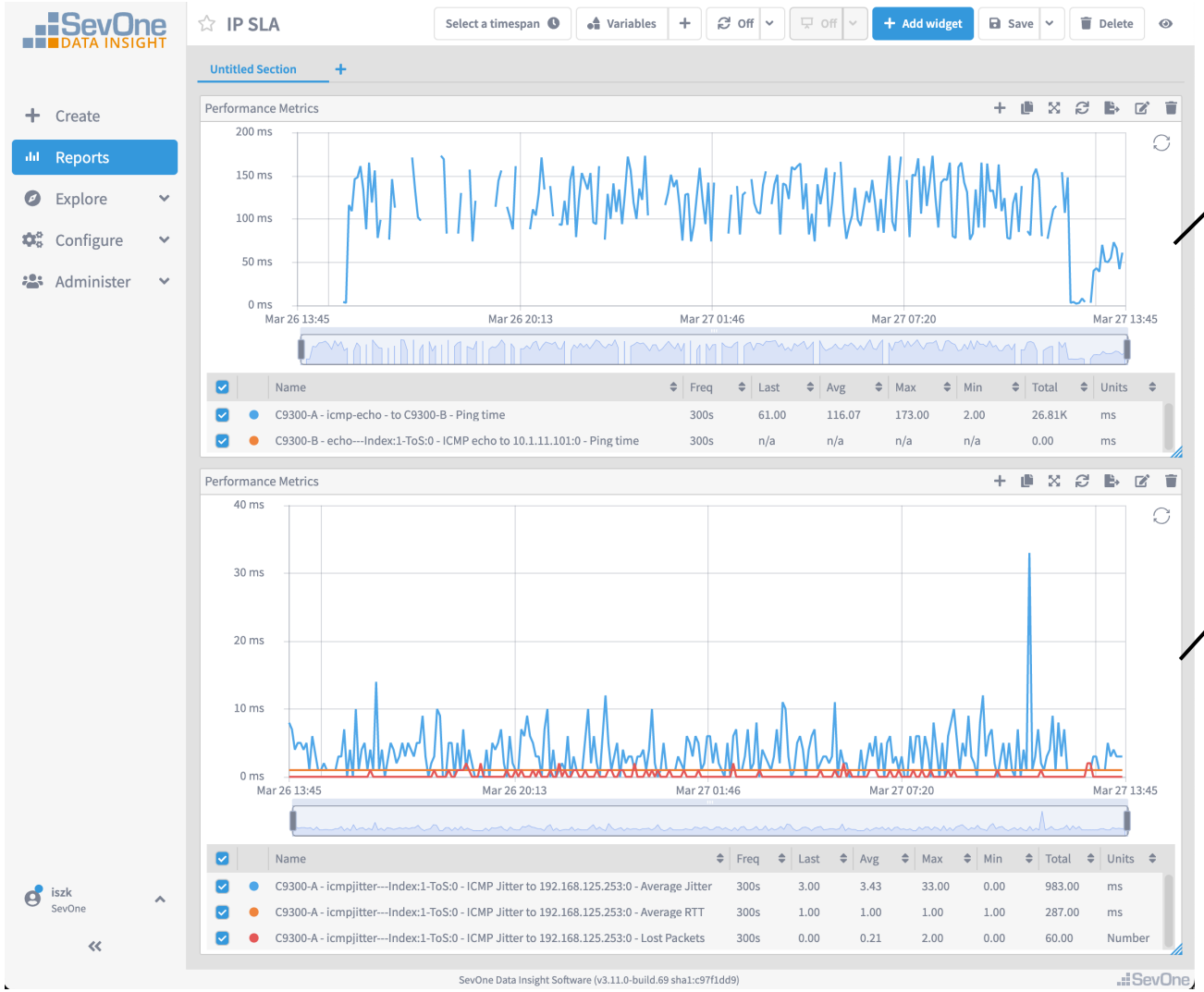
- SevOne NMS
  - icmp-jitter



©2022 IBM Corporation

3.2.3. IP SLAモニタリング (4/4)

- SevOne Data Insight (SDI)
  - IP SLA情報をダッシュボードのリソースとして使用可能



icmp-echoで得られるRTT

icmp-jitterで得られるジッタ平均、
RTT平均、パケットロス

©2022 IBM Corporation

3.3. NBAR (Network-Based Application Recognition)

NBAR概要

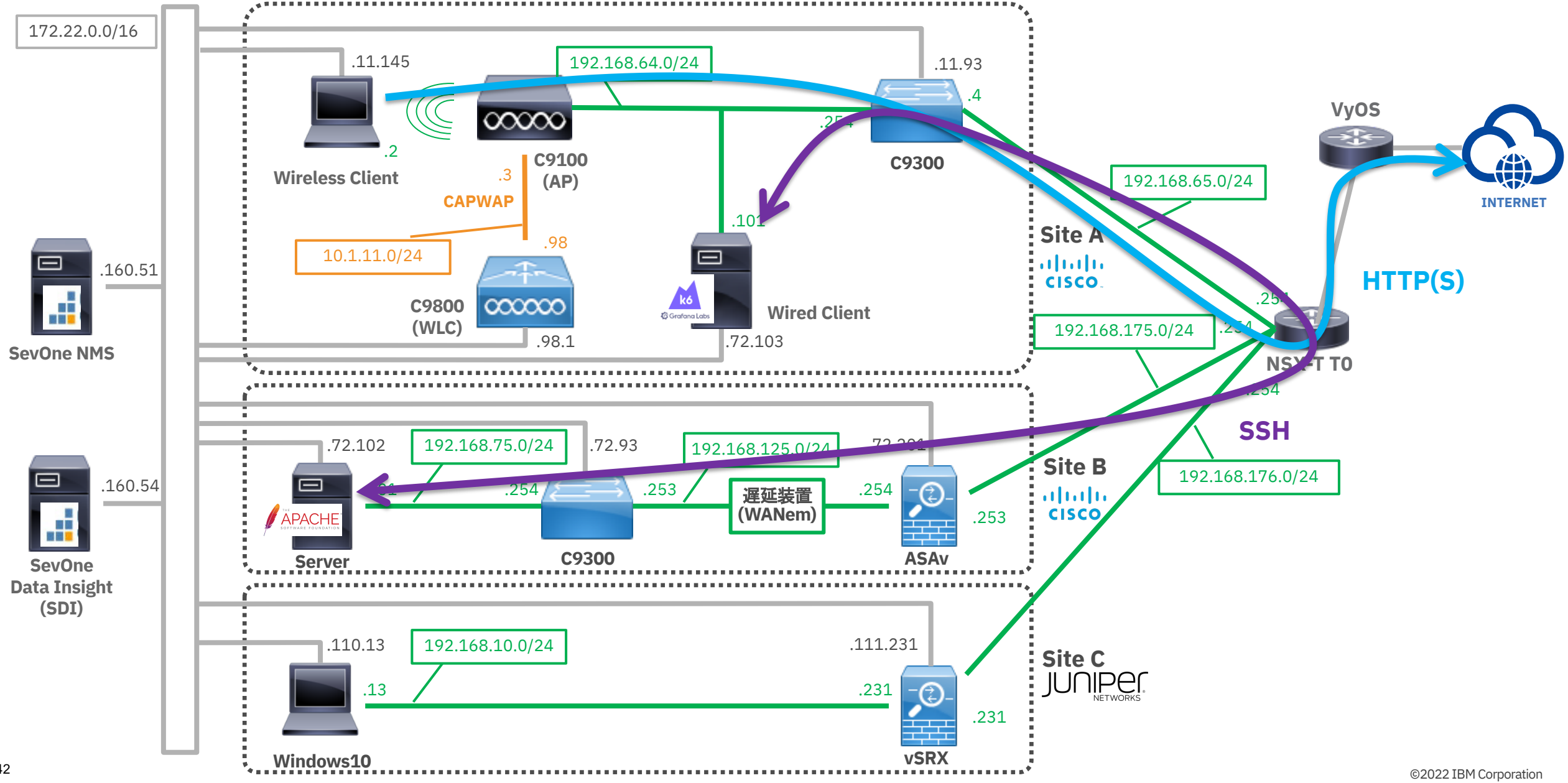
- NBARは、Cisco社が開発したネットワーク・トラフィックのプロトコルやアプリケーションを識別する技術で、Layer 3～7のアプリケーション分類が可能
- NBARを有効化したCiscoデバイスでインタフェースを流れるネットワーク・トラフィックのアプリケーションを識別し、どのアプリケーションでどれだけ帯域を使用したかを分析可能
- また、NetFlowと併用することで、例えば「Zoom」「Microsoft 365」「box」「youtube」などの動的なポートを用いるアプリケーションのフローの監視が可能となる
- SevOne NMSは、CiscoデバイスがNBAR情報をSNMPを使用して取得する

検証内容

- Ciscoスイッチを使用してNBARを有効化したインターフェースを経由するSSHセッションやHTTPセッションを発生させ、SevOneにてアプリケーション毎の Input / Output の帯域使用状況がモニタリングできることを確認する

©2022 IBM Corporation

3.3.1. 検証構成



©2022 IBM Corporation

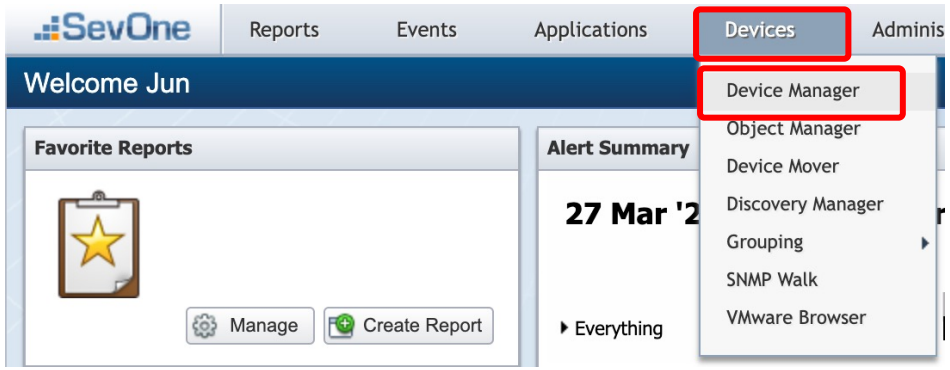
3.3.2. 設定

- 設定概要
  1. NBAR Monitoring有効化
  2. NBAR設定 (Ciscoデバイス)

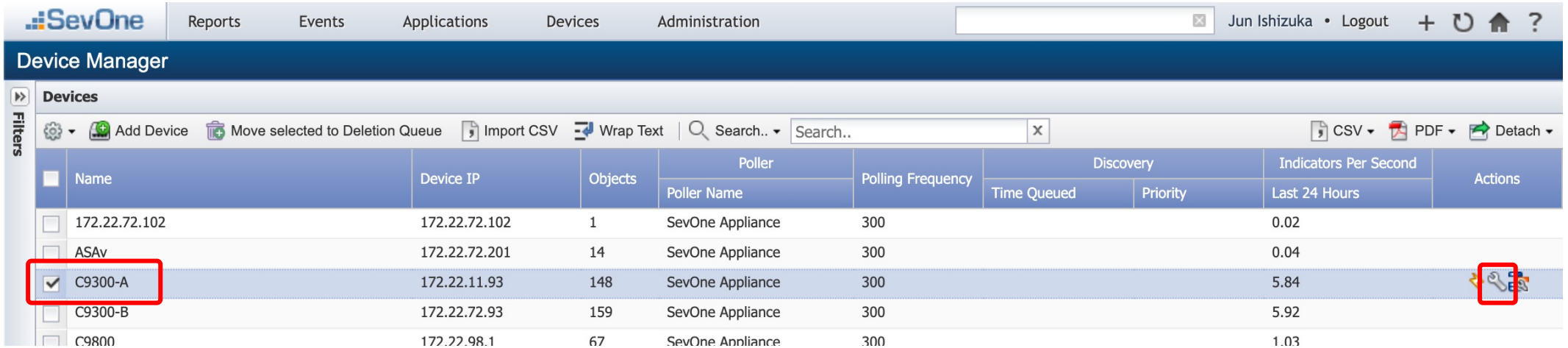
©2022 IBM Corporation

3.3.2.1. NBAR Monitoring有効化 (1/2)

- 管理デバイスのNBAR Monitoring有効化
  - メニュー・バーより、[Devices] > [Device Manager] を選択



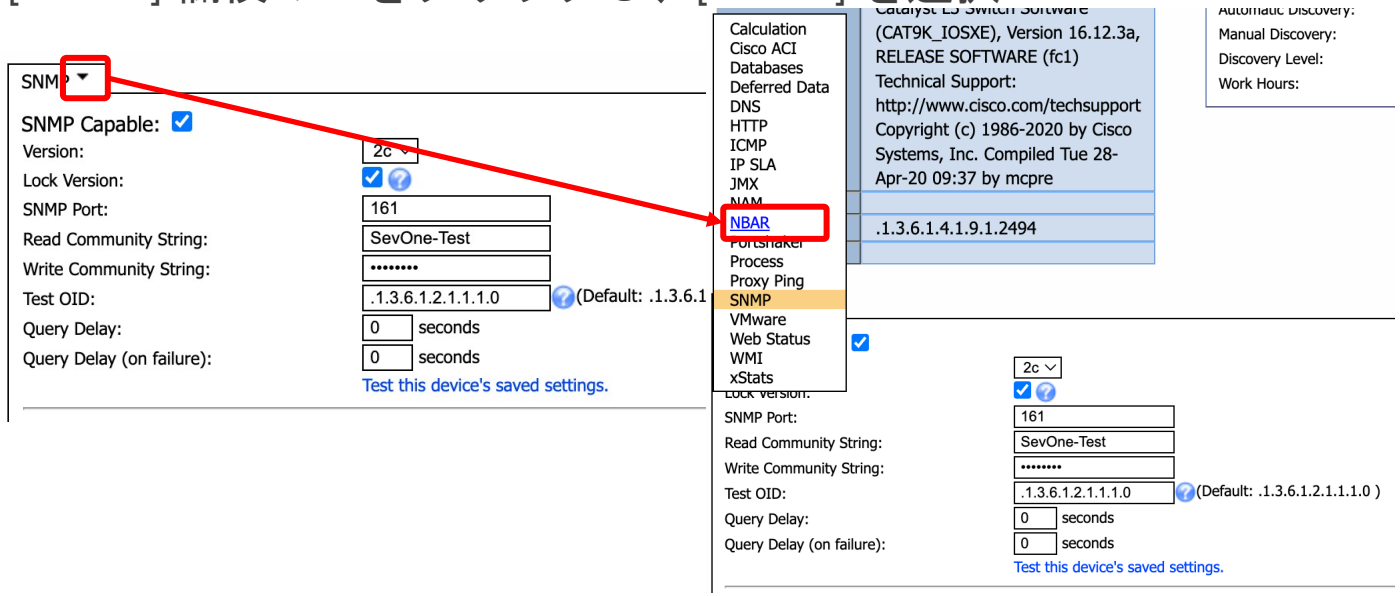
  - 対象デバイスを選択し、[Actions] 列真ん中の [Edit this device] アイコンを選択



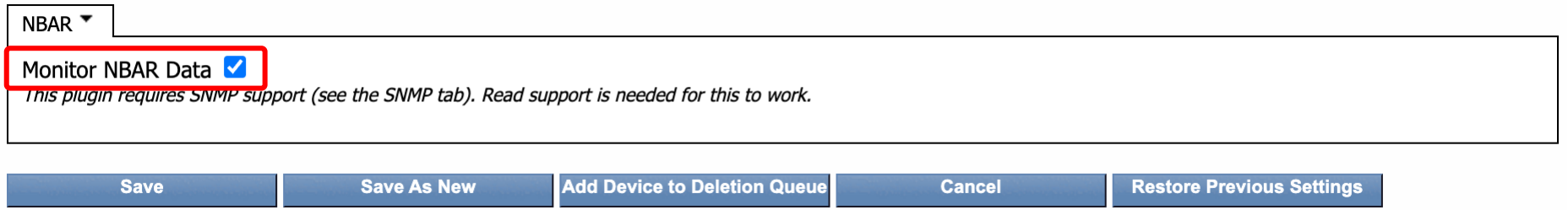
©2022 IBM Corporation

3.3.2.1. NBAR Monitoring有効化 (2/2)

– [SNMP] 欄横の▼をクリックし、[NBAR] を選択



– [Monitor NBAR Data] にチェックが付いていることを確認



©2022 IBM Corporation

3.3.2.2. NBAR設定 (Ciscoデバイス)

- Cisco機器のコマンドラインでNBARを設定

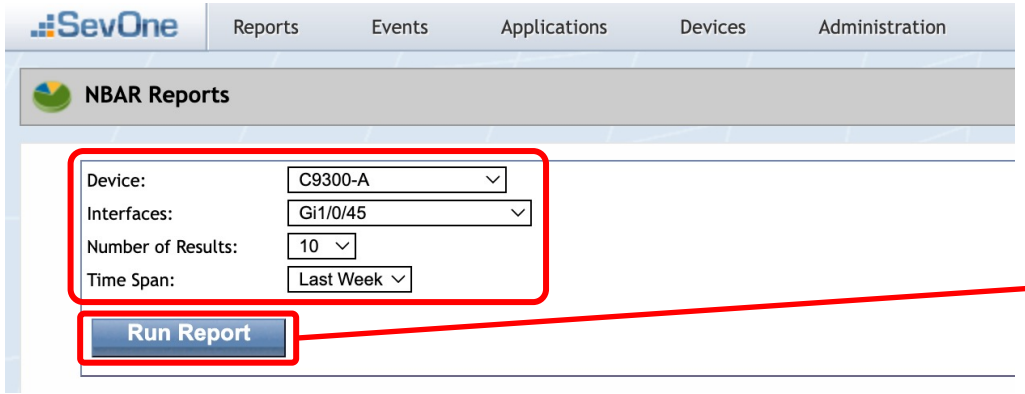
```
C9300-A#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
C9300-A(config)#int ra gi1/0/47, gi1/0/45
C9300-A(config-if-range)#ip nbar protocol-discovery
C9300-A(config-if-range)#end
```

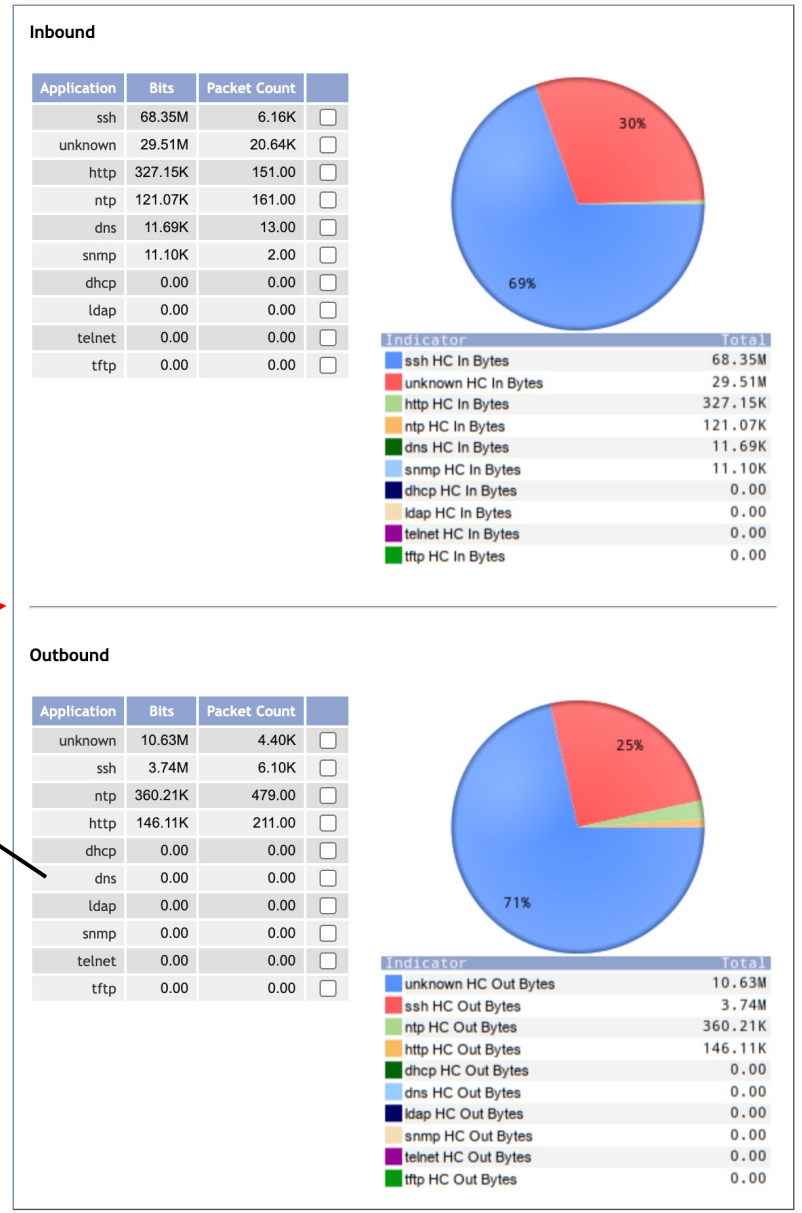
```
C9300-A#sh ip nbar protocol-discovery int gi1/0/45

GigabitEthernet1/0/45

Last clearing of "show ip nbar protocol-discovery" counters 1w6d


                        Input                  Output
                        -----                  ------
Protocol                     Packet Count          Packet Count
                        Byte Count            Byte Count
                        5min Bit Rate (bps)     5min Bit Rate (bps)
                        5min Max Bit Rate (bps)  5min Max Bit Rate (bps)
---------------------------- ---------------------- ------------------------
ms-services                   864202                440011
                        1123774833             26485467
                        0                  0
                        3050000                75000
youtube                     466896                261596
                        559732187              32100315
                        0                  0
                        659000                 30000
binary-over-http          15787                 8145
                        20436155               512663
                        0                  0
                        232000                 12000
ssh                         15963                 15829
                        22392120               1208694
                        0                  0
                        82000                  6000

(省略)
```


©2022 IBM Corporation

3.3.3. NBARモニタリング

- SevOne NMSのNBAR Reports
  - メニュー・バーより、[Applications] > [NBAR Reports] を選択
  - NBARが有効化されたCiscoデバイスのインターフェース、レポートに表示する結果数、期間を選択し、[Run Report] ボタンを押下





対象インターフェースの In/Out
それぞれでアプリケーション毎の
bit数、パケット数を確認可能

©2022 IBM Corporation

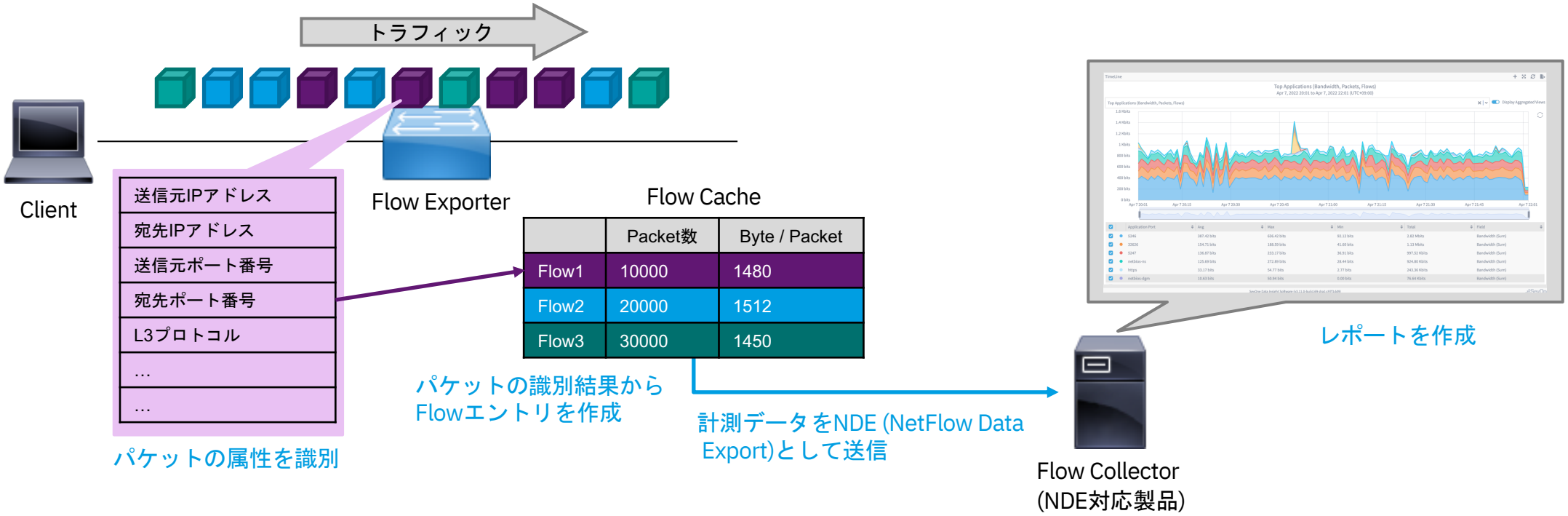
3.4. xFlow (1/2)

■ NetFlow概要

– Flowとは

- ネットワーク装置を通過する、共通の属性をもった一方通行の連続したパケットのこと
- 共通の属性とは、例えば、送信元/送信先IPアドレスやポート番号、入力インターフェースなど

– NetFlowのアーキテクチャ



©2022 IBM Corporation

(参考) xFlow 比較

- NetFlow
  - Cisco社が開発
  - 基本的に全てのパケットを観測してFlow Dataを生成（パケットのサンプリングはオプション設定）
  - version 5, version 9 が主流
  - version 5 は測定内容 (フィールド) が固定されているが、version 9 はテンプレートベースとなっておりフィールドを自由に決められる

- sFlow
  - 一部のパケットを観測してFlow Dataを生成（パケットのサンプリングが前提）
  - InMon社が開発し、複数のベンダーでサポート

- IPFIX
  - NetFlow version 9をもとに標準化されたもの (NetFlow version 10)

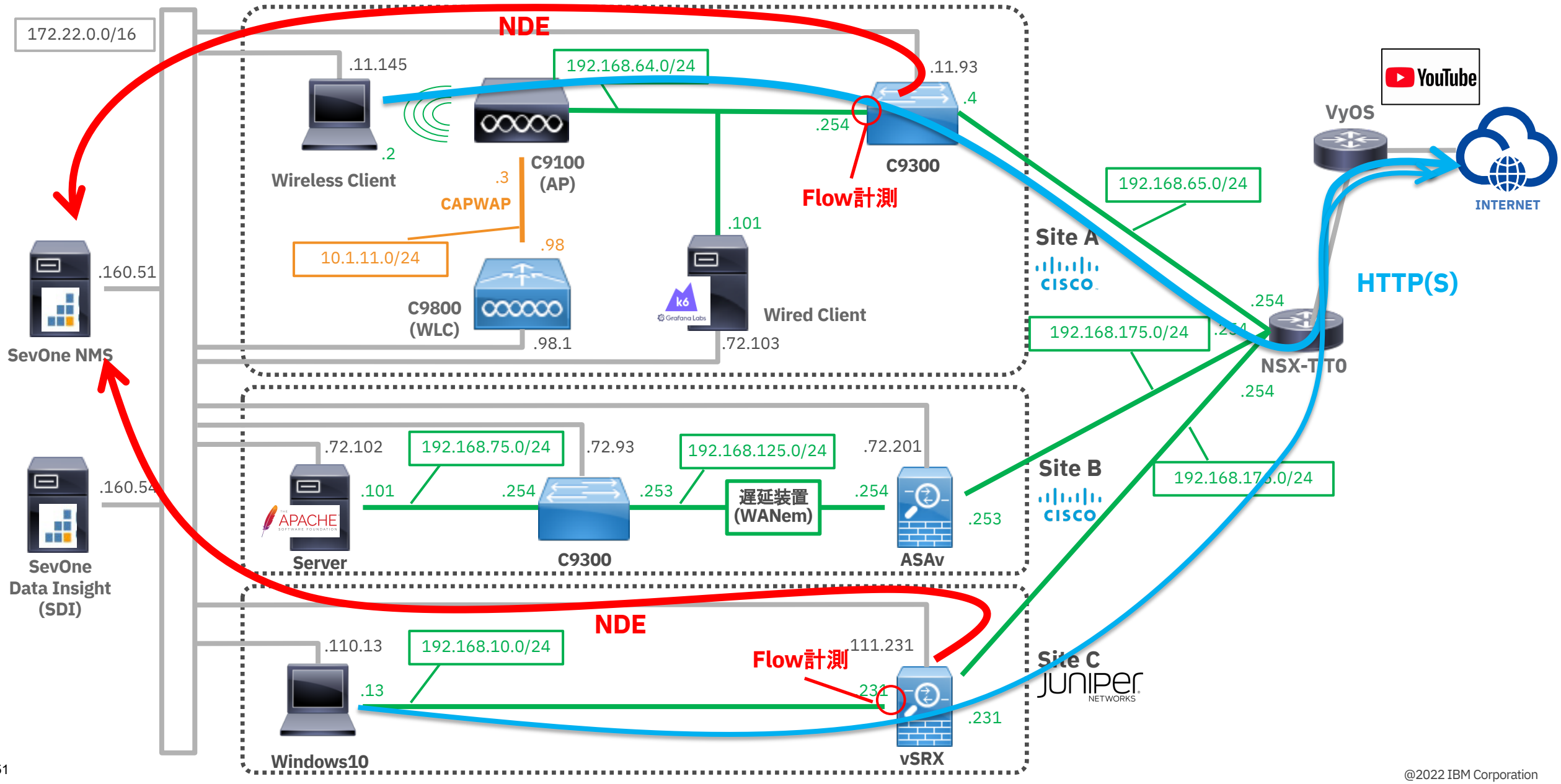
©2022 IBM Corporation

3.4. xFlow (2/2)

- 検証内容
  - NMSがFlow Collectorとして、どのようなネットワークの観測ができるか確認する
    - Flow Dataのソースとしては、CiscoのNetFlow version 9を使用する
  - NBARと組み合わせた場合に、Flow Reportへアプリケーション識別が反映されることを確認する

©2022 IBM Corporation

3.4.1. 検証構成



@2022 IBM Corporation

3.4.2. セットアップ

■ 設定概要

1. デバイスの設定 (Ciscoデバイス)
   - Catalyst 9300 Sample Config
   - vSRX Sample Config
2. NMSの設定
   - NDE受信の設定
   - Flow Report Viewの設定

©2022 IBM Corporation

3.4.2.1. デバイスの設定 (Ciscoデバイス)

- Catalyst 9300 Sample Config

```
flow record LANCOPE1_IN
 match ipv4 version
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match interface input
 match application name
 collect interface output
 collect counter bytes long
 collect counter packets long
 collect timestamp absolute first
 collect timestamp absolute last

flow exporter SEVONE
 destination 172.22.160.51
 source Vlan172
 transport udp 9996

flow monitor IPv4_NETFLOW
 exporter SEVONE
 cache timeout active 60
 record LANCOPE1_IN

interface GigabitEthernet1/0/47
 ip flow monitor IPv4_NETFLOW input
```

match application name → アプリケーション識別を有効にするための設定

transport udp 9996 → NMSの受信ポートデフォルト
- Non-Sampled : UDP 9996 (Cluster Settingsで変更可能)
- Sampled : UDP 6343

©2022 IBM Corporation

3.4.2.1. デバイスの設定 (Juniperデバイス)

- vSRX Sample Config

```
set services flow-monitoring version-ipfix template ipv4-template flow-active-timeout 60
set services flow-monitoring version-ipfix template ipv4-template flow-inactive-timeout 70
set services flow-monitoring version-ipfix template ipv4-template template-refresh-rate seconds 30
set services flow-monitoring version-ipfix template ipv4-template option-refresh-rate seconds 30
set services flow-monitoring version-ipfix template ipv4-template ipv4-template

set interfaces ge-0/0/1 unit 0 family inet sampling input
set interfaces ge-0/0/1 unit 0 family inet sampling output

set forwarding-options sampling instance s1 input rate 100
set forwarding-options sampling instance s1 family inet output flow-server 172.22.160.51 port 9996
set forwarding-options sampling instance s1 family inet output flow-server 172.22.160.51 version-ipfix template ipv4-template
set forwarding-options sampling instance s1 family inet output inline-jflow source-address 172.22.111.231
```

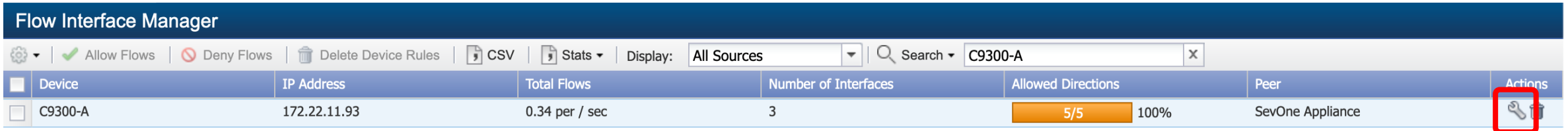
IPFIX テンプレートの設定

NMS の受信ポート UDP 9996

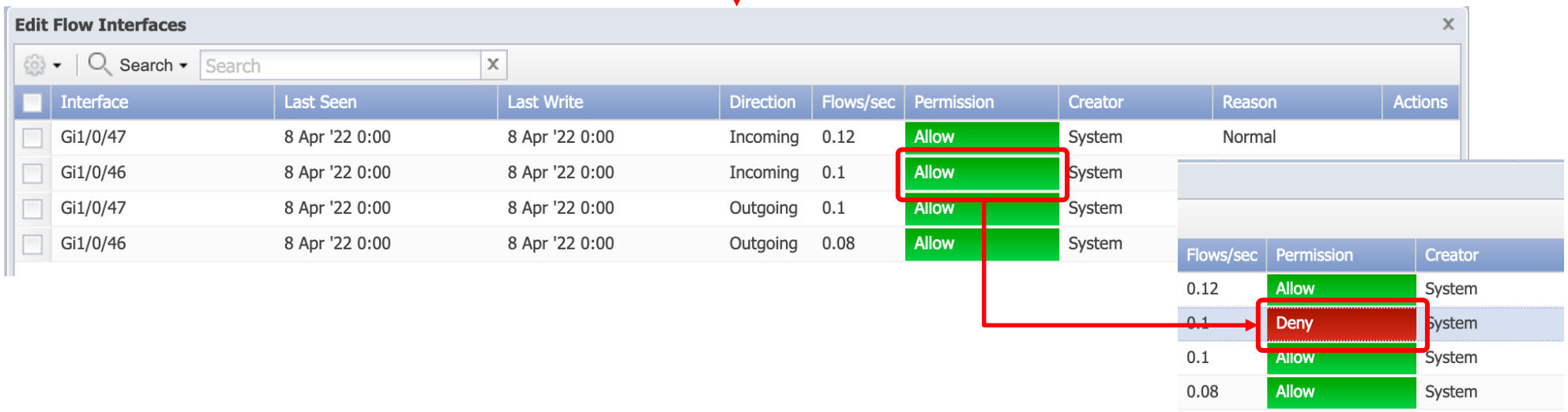
©2022 IBM Corporation

3.4.2.2. NMSの設定 (1/5)

- NDE受信の設定
  - デバイスからNDEを受信すると、[Administration] > [Flow Configuration] > [Flow Interface Manager] の画面にて、そのデバイスが表示される



  - [Action] 列の [Edit Interfaces] を押下するとflow monitorを設定しているInterfaceが表示される
    Permissionの部分を押下することで、そのInterfaceからのNDE受信の許可/拒否を切り替え可能



©2022 IBM Corporation

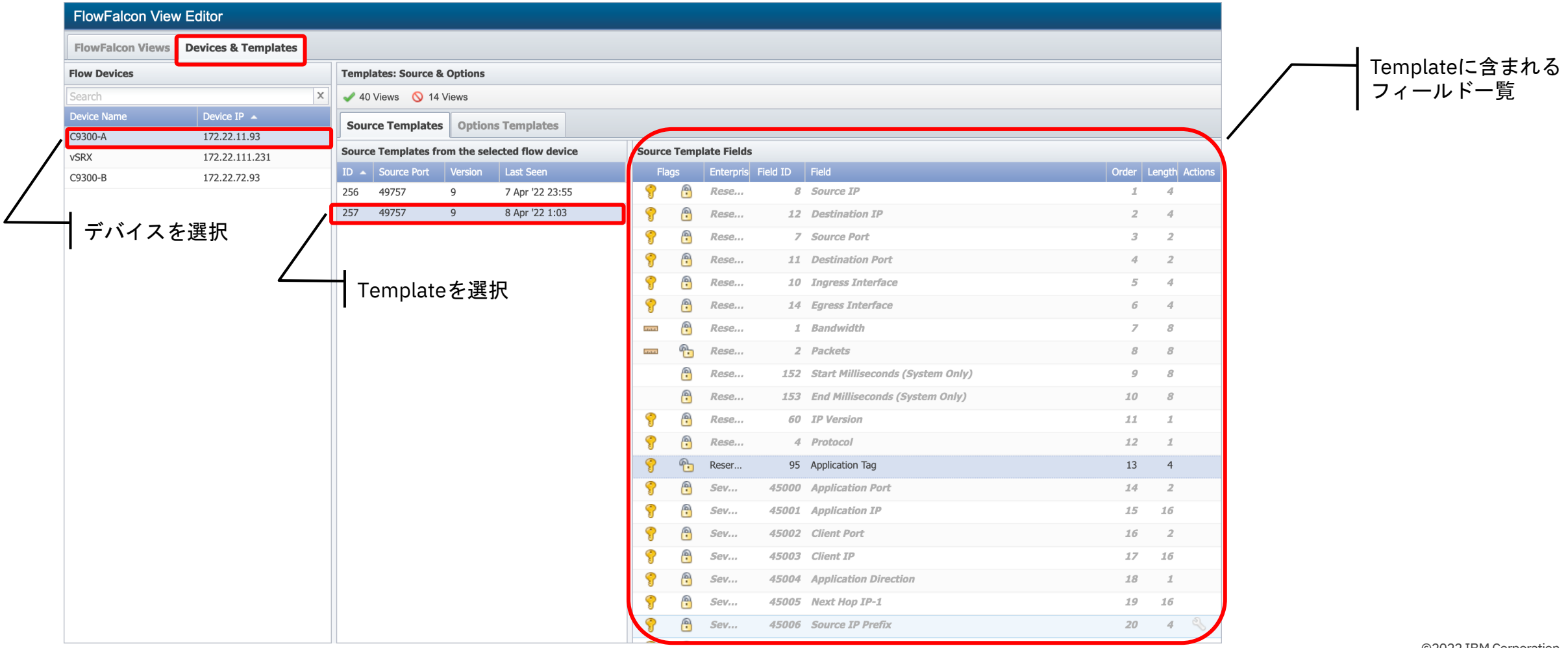
3.4.2.2. NMSの設定 (2/5)

- Flow Report Viewの設定
  - デバイスが送信してくるflow templateのフィールドのうち、どのフィールドを使用してFlow Reportの作成をするかカスタマイズすることが可能
  - Flow Reportにてどのフィールドを使用するかの定義のセットは、Viewという名前で呼ばれる
  - Viewの作成・編集は [Administration] > [Flow Configuration] > [FlowFalcon View Editor] の画面にて実施
  - NMSで定義したViewはSDIにも反映され、使うことが可能

©2022 IBM Corporation

3.4.2.2. NMSの設定 (3/5)

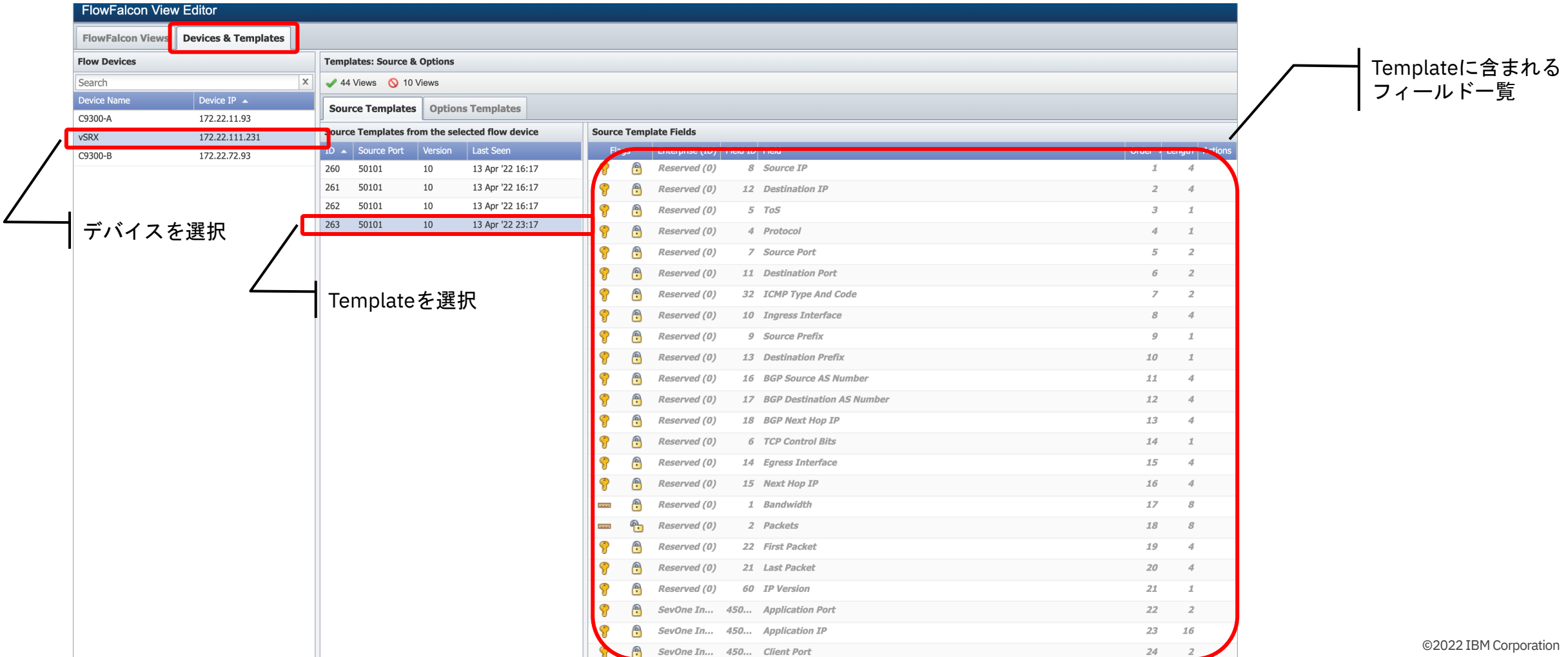
- FlowFalcon View Editor
  - [Devices & Template] タブ
    - デバイスが送付してくるflow templateに含まれるフィールドを確認可能



©2022 IBM Corporation

(参考) NMSの設定 (Juniper)

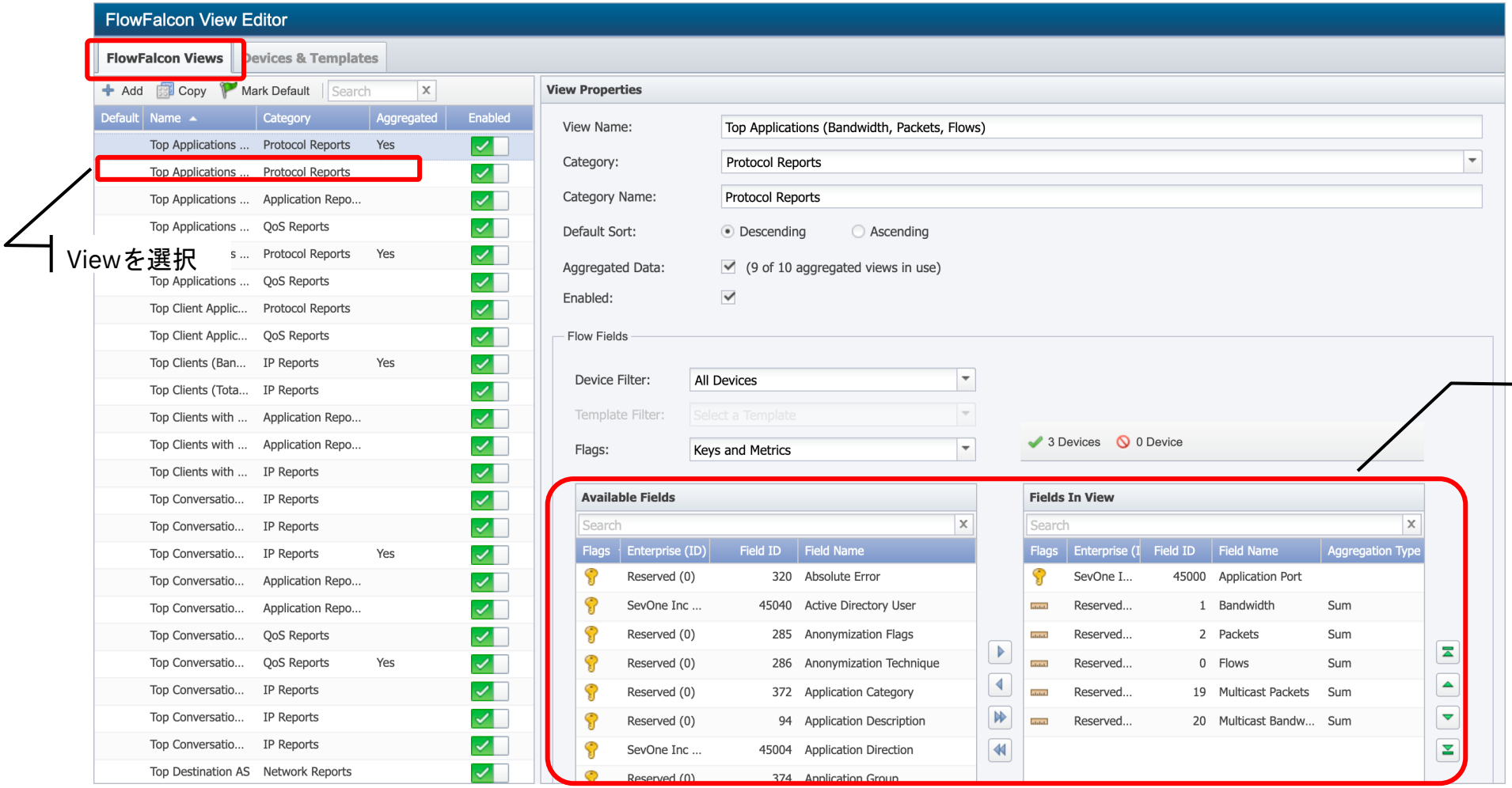
- FlowFalcon View Editor
  - [Devices & Template] タブ
    - デバイスが送付してくるflow templateに含まれるフィールドを確認可能



©2022 IBM Corporation

3.4.2.2. NMSの設定 (4/5)

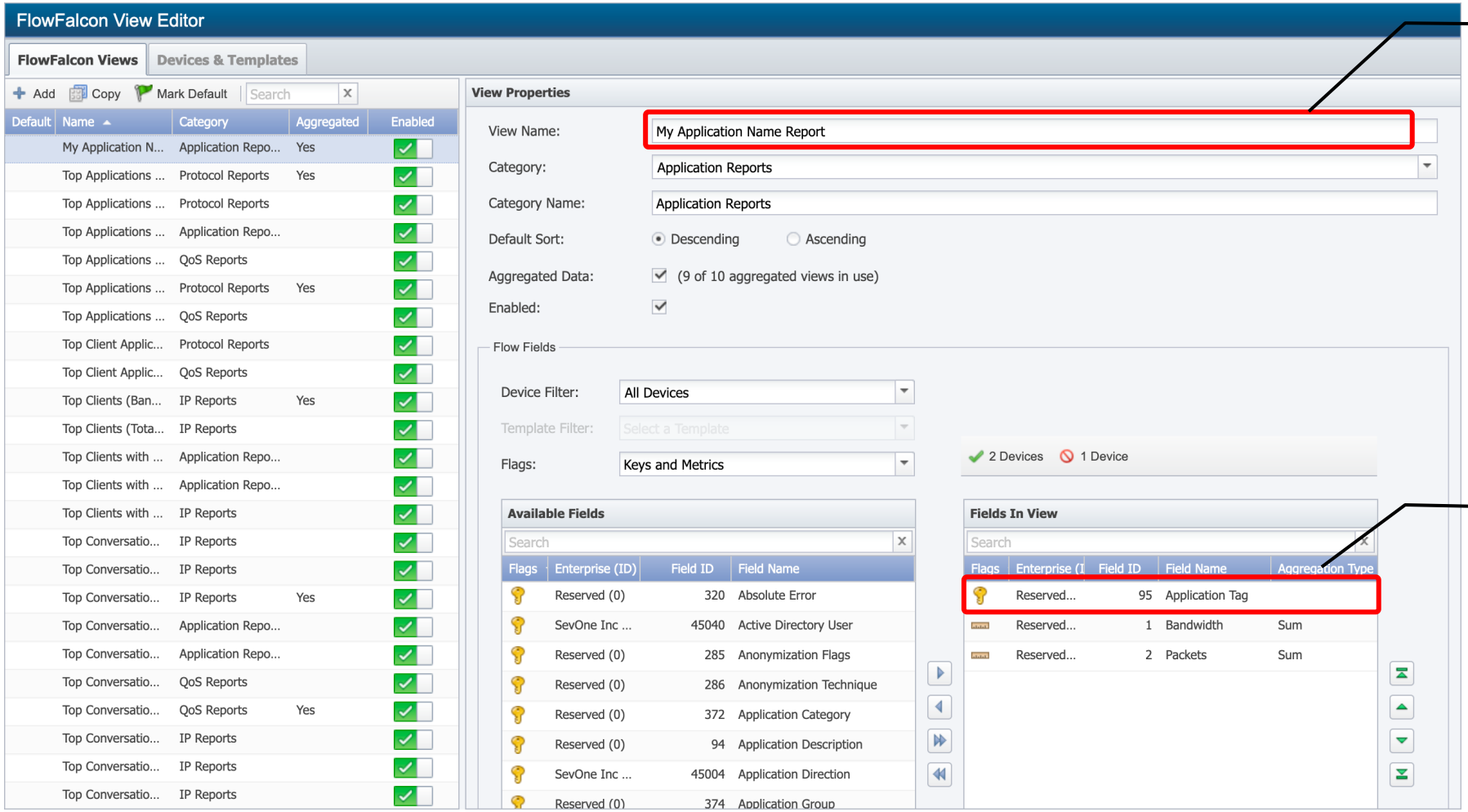
- FlowFalcon View Editor
  - [FlowFalcon View] タブ
    - Viewの作成や編集が可能（初期状態でいくつかのViewが用意されている）



©2022 IBM Corporation

3.4.2.2. NMSの設定 (5/5)

- NBARによるアプリケーション識別を反映させたViewの作成
  - デフォルトではNBARによるアプリケーション識別を反映させたViewは存在しない
  - Application Tagというフィールドを使用するViewを作成する



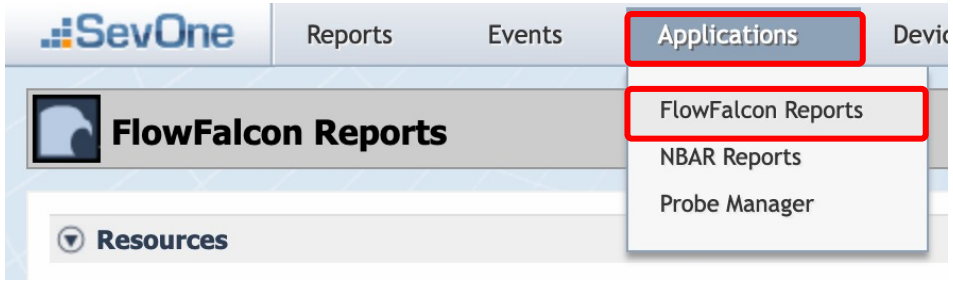
任意の名前で作成

Application Tagのフィールドを使うことで、NBARによって識別されたアプリケーション名をレポートに表示できる

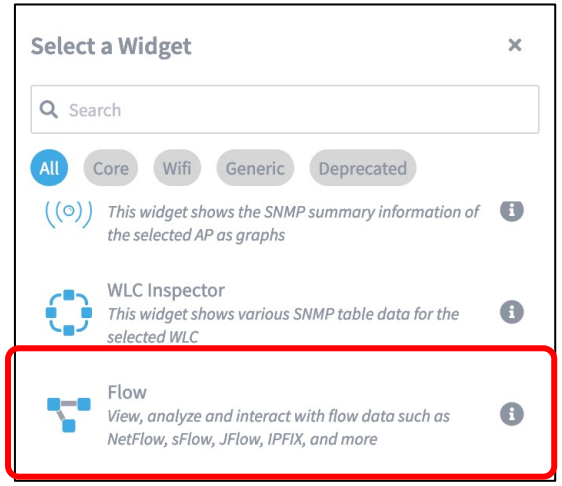
©2022 IBM Corporation

3.4.2.3. Flow Reportの表示

- NMSでFlow Reportを出力する場合は以下のメニューにアクセス
  - [Application] > [Flow Falcon Reports]



- SDIでFlow Reportを出力する場合は、FlowのWidgetを使用する

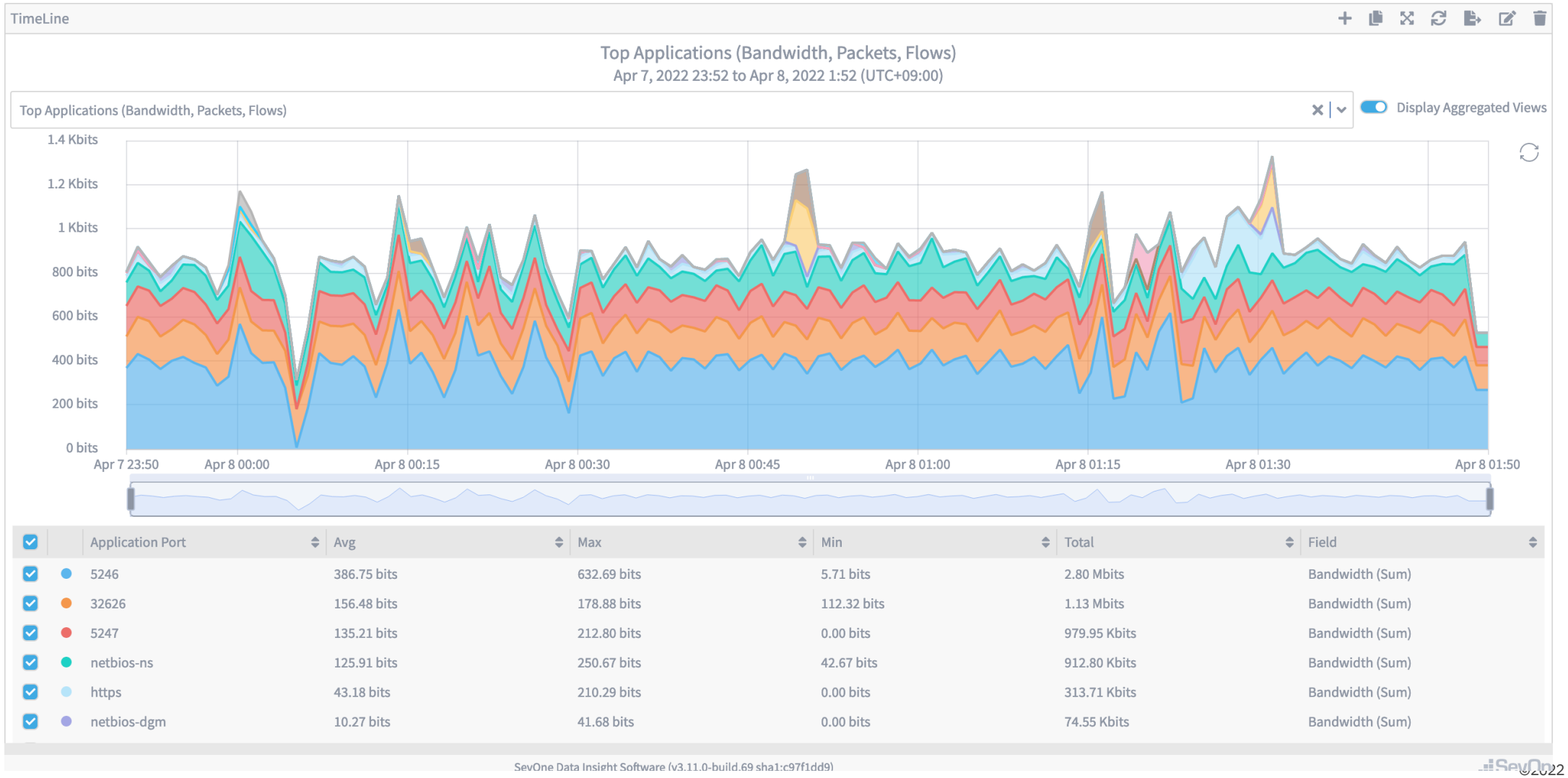


- 得られる結果はどちらでも変わらないが、以降のページはUIが優れているSDIのレポートを紹介

©2022 IBM Corporation

3.4.2.3.1. SDIにおけるFlow Report (1/3)

- TimeLineチャート
  - 特定のプロトコルに対してトラフィック量の遷移を観測するなどの用途が考えられる

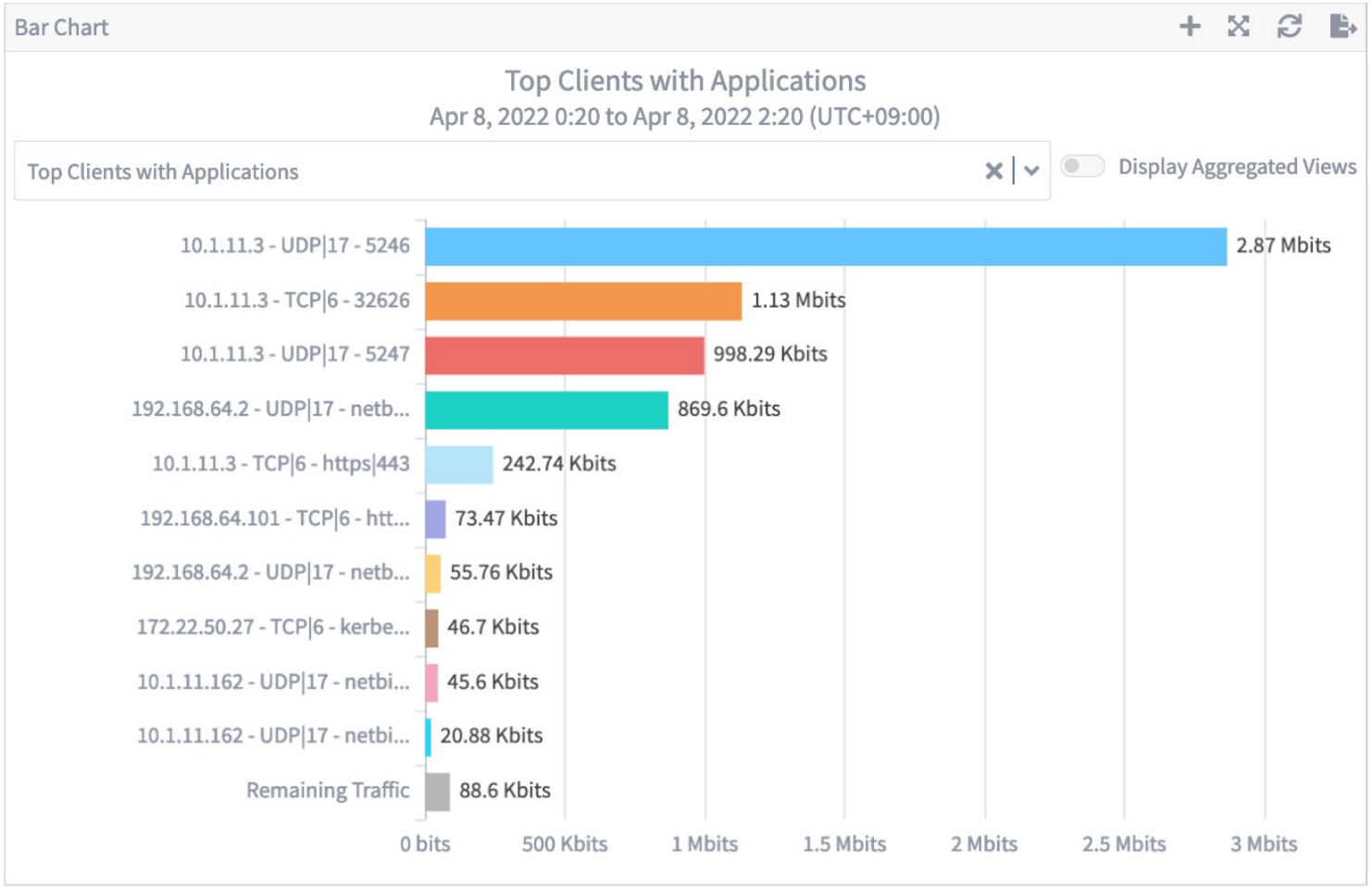


Application Port	Avg	Max	Min	Total	Field
5246	386.75 bits	632.69 bits	5.71 bits	2.80 Mbits	Bandwidth (Sum)
32626	156.48 bits	178.88 bits	112.32 bits	1.13 Mbits	Bandwidth (Sum)
5247	135.21 bits	212.80 bits	0.00 bits	979.95 Kbits	Bandwidth (Sum)
netbios-ns	125.91 bits	250.67 bits	42.67 bits	912.80 Kbits	Bandwidth (Sum)
https	43.18 bits	210.29 bits	0.00 bits	313.71 Kbits	Bandwidth (Sum)
netbios-dgm	10.27 bits	41.68 bits	0.00 bits	74.55 Kbits	Bandwidth (Sum)

©2022 IBM Corporation

3.4.2.3.1. SDIにおけるFlow Report (2/3)

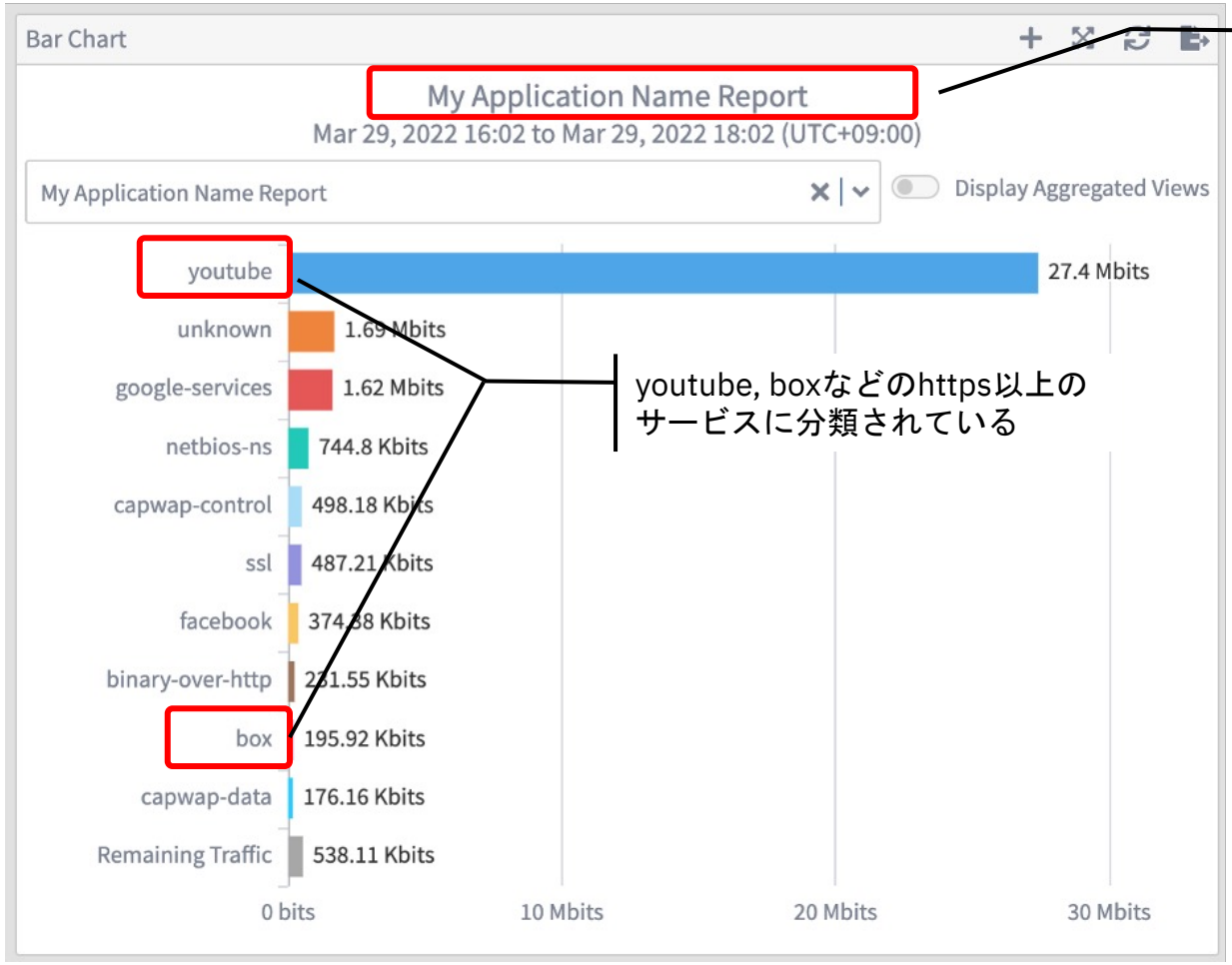
- Barチャート
  - トラフィック量の多いクライアント - アプリケーション通信を把握するなどの用途が考えられる



©2022 IBM Corporation

3.4.2.3.1. SDIにおけるFlow Report (3/3)

- NBARによるアプリケーション識別が有効であるView
  - 先ほどのページはhttps以上の情報が取得できていないが、こちらで作成したViewでは、youtube, boxなどのサービス名ごとにFlowが分類されている



Flow Reportに適用されている
Viewの名前

youtube, boxなどのhttps以上の
サービスに分類されている

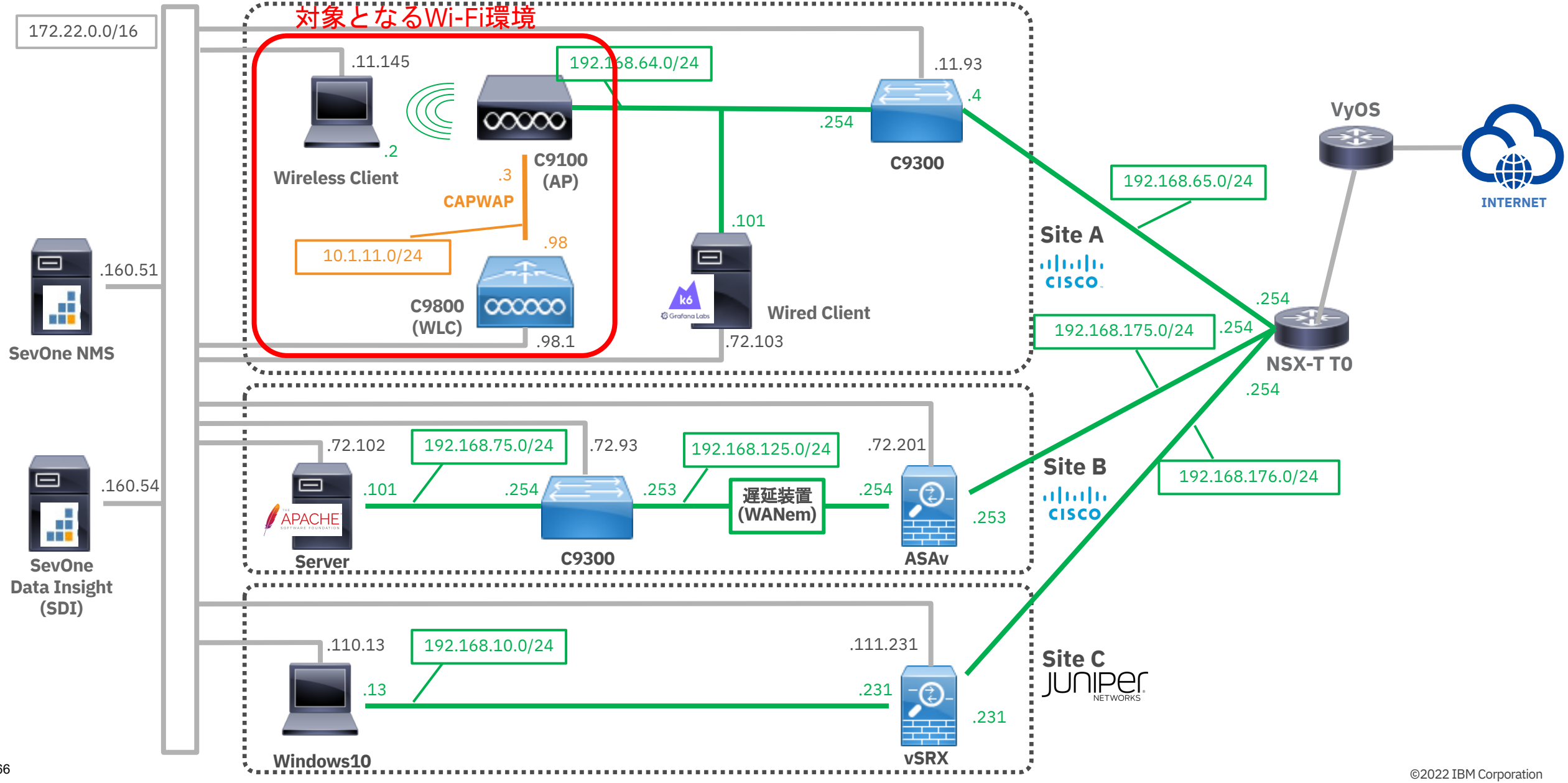
©2022 IBM Corporation

3.5. Wi-Fi

- 検証内容
  - SevOne NMSにWireless LAN Controller (WLC) Collectorをインストールし、Wi-Fi環境のモニタリングができることを確認する

©2022 IBM Corporation

3.5.1. 検証構成



©2022 IBM Corporation

3.5.1. Wireless LAN Controller (WLC) Collector

- SevOne NMSでWi-Fi環境のモニタリングを行うためには、Wireless LAN Controller (WLC) Collector (Wi-Fi Collectorとも言う) が必要
- WLC CollectorはNMSアプライアンスで共同ホストされるコンテナイメージ
  - NMS上で動作させることも、hostネットワーク・モードのリモートVM上で動作させることも可能
  - 当資料ではNMS上にインストールして使用する
- SNMPを使用してWi-Fiデータを取得する

©2022 IBM Corporation

3.5.2. WLC Collectorのセットアップ

■ 前提

– Wireless LAN Controller (WLC)がNMSのDevice Managerに登録されていること

– WLC Collectorのイメージ・ファイルを入手すること

- 当資料では以下のファイルを使用
- WLC CollectorはNMS上、Wi-Fi widgetはSDI上の任意のディレクトリーにそれぞれ配置

wifi-solution-v2.9.0-build-174642.tar.gz wifi-solution-v2.9.0-build-174642.tar.gz.sha256sum.txt	NMS用 WLC Collector
wifi-sdi-widgets-2.9.0-build-174977.tar wifi-sdi-widgets-2.9.0-build-174977.sha256.txt	SDI用 Wi-Fi widget

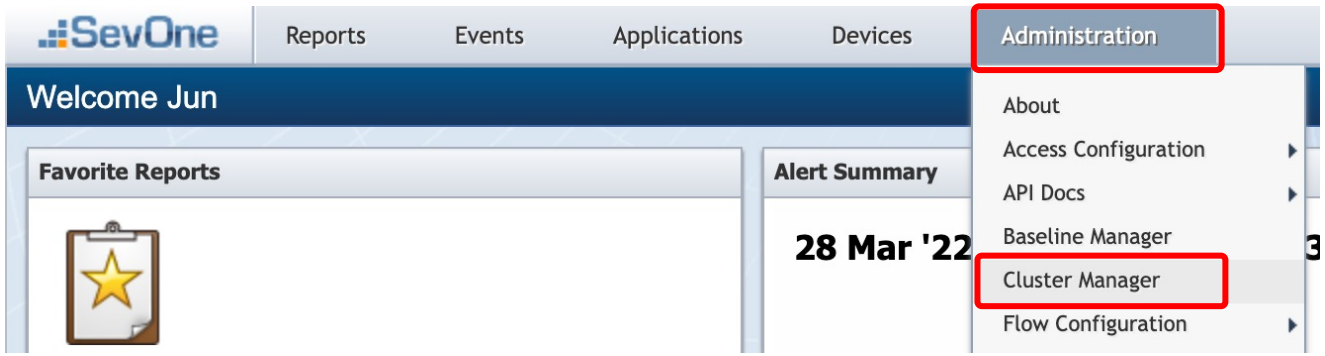
■ 手順概要

1. 事前準備
   - WLC CollectorのInstallation Guideの記載に従い、NMSで [Mask Read Community String] を無効化
2. WLC Collectorのインストール
3. WLC Collectorの起動

©2022 IBM Corporation

3.5.2.1. 事前準備 (1/2)

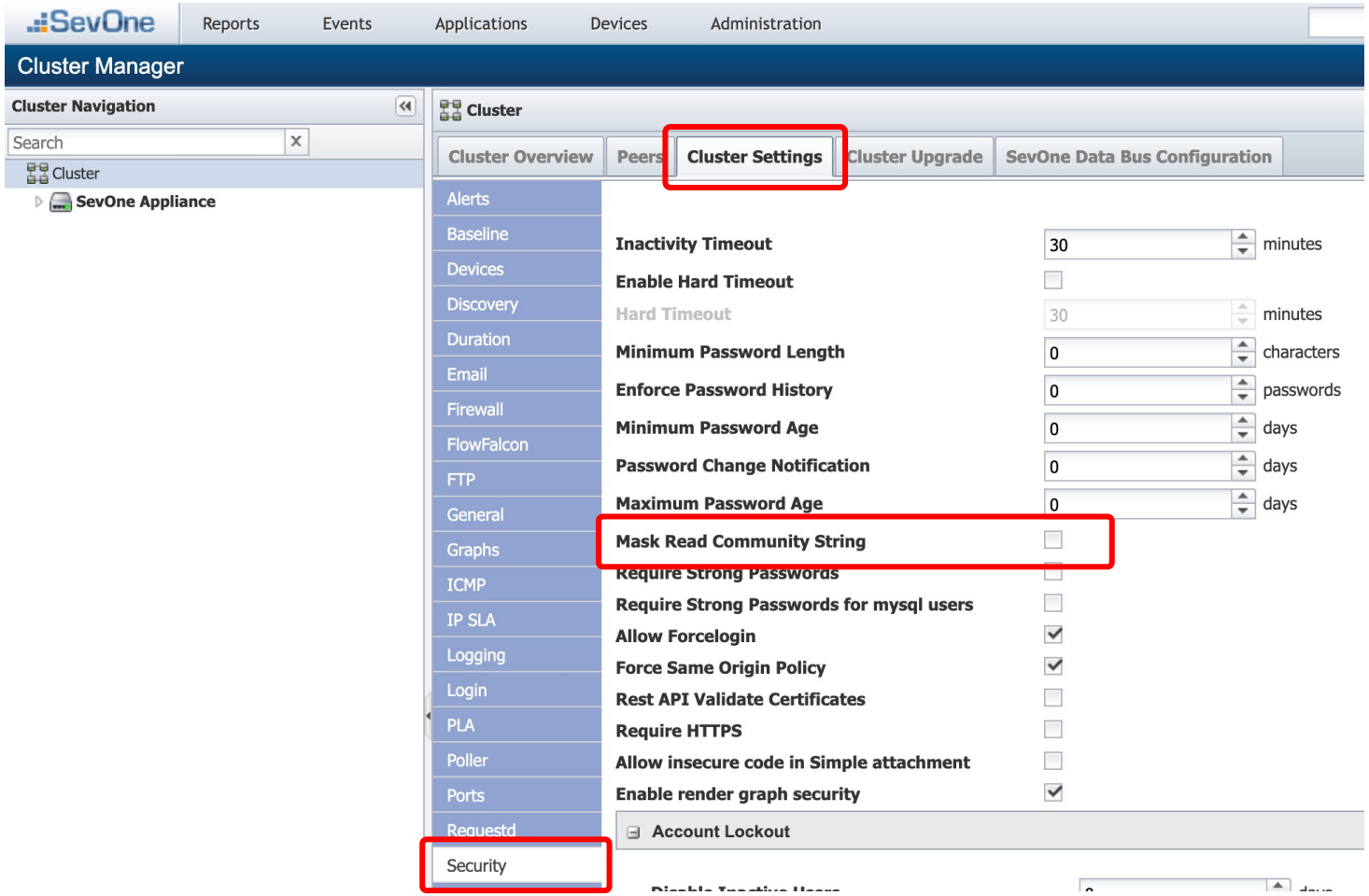
- WLC CollectorのInstallation Guideの記載に従い、NMSで [Mask Read Community String] を無効化
  - NMSにログインし、[Administration] > [Cluster Manager] を選択



©2022 IBM Corporation

3.5.2.1. 事前準備 (2/2)

- NMSで [Mask Read Community String] を無効化
  - [Cluster Settings] タブのメニューより、[Security] を選択し、[Mask Read Community String] のチェックを外して保存



©2022 IBM Corporation

3.5.2.2. WLC Collectorのインストール (1/6)

- NMSにrootユーザーでSSHログインし、イメージ・ファイルを解凍する

```
root@sevone-nms:~/wifi [6.1.0] [15:08:21] $ ls -la
合計 292480
drwxr-xr-x. 2 root root      202  3月  9 15:08 .
dr-xr-x---. 5 root root      182  3月  9 15:08 ..
-rw-r--r--. 1 root root 299493267  3月  9 15:06 wifi-solution-v2.9.0-build-174642.tar.gz
-rw-r--r--. 1 root root      110  3月  9 15:06 wifi-solution-v2.9.0-build-174642.tar.gz.sha256sum.txt

root@sevone-nms:~/wifi [6.1.0] [15:08:51] $ tar xvf wifi-solution-v2.9.0-build-174642.tar.gz
wifi-solution-v2.9.0-build-174642/
wifi-solution-v2.9.0-build-174642/upgrade.sh
wifi-solution-v2.9.0-build-174642/install.sh
wifi-solution-v2.9.0-build-174642/WifiSolution-ootb-reports-NMS.spk
wifi-solution-v2.9.0-build-174642/multi-peer-installer.tar.gz
wifi-solution-v2.9.0-build-174642/wifi-v2.9.0-build-174642.tar.gz
root@sevone-nms:~/wifi [6.1.0] [15:09:04] $
```


©2022 IBM Corporation

3.5.2.2. WLC Collectorのインストール (2/6)

- 解凍したディレクトリーにsha256 checksumのtextファイルを配置し、"./install.sh setup" を実行

```
root@sevone-nms:~/wifi [6.1.0] [15:09:29] $ mv wifi-solution-v2.9.0-build-174642.tar.gz.sha256sum.txt wifi-solution-v2.9.0-build-174642
root@sevone-nms:~/wifi [6.1.0] [15:09:52] $ cd wifi-solution-v2.9.0-build-174642/
root@sevone-nms:~/wifi/wifi-solution-v2.9.0-build-174642 [6.1.0] [15:10:02] $ ls -la
合計 293704
drwxr-xr-x. 2 root root      219  3月 14 17:00 .
drwxr-xr-x. 4 root root      138  3月 14 17:07 ..
-rw-r--r--. 1 root root    40038  1月 25 12:11 WifiSolution-ootb-reports-NMS.spk
-rwxr-xr-x. 1 root root    22026  1月 25 12:11 install.sh
-rw-r--r--. 1 root root     8443  1月 25 12:11 multi-peer-installer.tar.gz
-rwxr-xr-x. 1 root root     3540  1月 25 12:11 upgrade.sh
-rw-r--r--. 1 root root      110  3月  9 15:06 wifi-solution-v2.9.0-build-174642.tar.gz.sha256sum.txt
-rw-r--r--. 1 root root 300666515  1月 25 12:11 wifi-v2.9.0-build-174642.tar.gz
root@sevone-nms:~/wifi/wifi-solution-v2.9.0-build-174642 [6.1.0] [15:10:04] $
root@sevone-nms:~/wifi/wifi-solution-v2.9.0-build-174642 [6.1.0] [15:14:36] $ ./install.sh setup
Do you want to backup your data at /opt/WLCCollector?(yes | no): yes
Verifying checksum of the collector tar.
Verification of the collector tar is successful.
OK: User is root.
OK: All the prerequisite requirements met
OK: NMS Version met minimum requirement of 5.7.2.32
OK: Docker version met minimum requirement of 18.06.1 and docker service is up and running.
OK: All files are present at /root/wifi/wifi-solution-v2.9.0-build-174642
-----------------------------------------
Setup
-----------------------------------------
OK: tar extracted successfully at /opt/WLCCollector
OK: Loaded vendor docker images
OK: Setup completed successfully
-----------------------------------------
root@sevone-nms:~/wifi/wifi-solution-v2.9.0-build-174642 [6.1.0] [15:15:18] $
```


©2022 IBM Corporation

3.5.2.2. WLC Collectorのインストール (3/6)

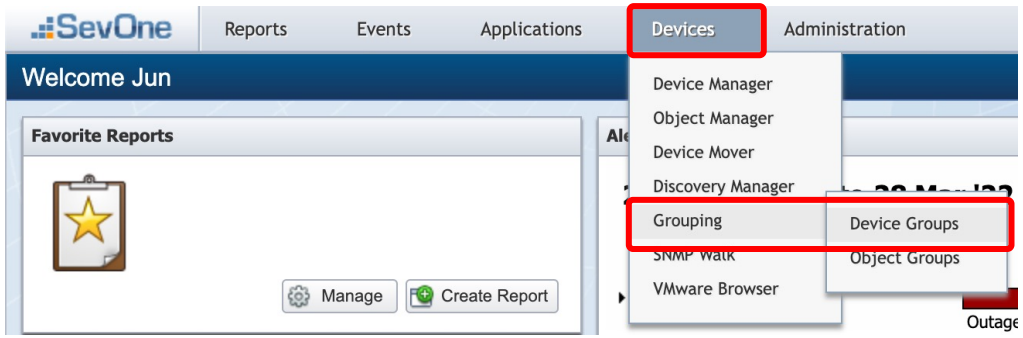
- 生成されたCisco WLC用の環境ファイル (cisco.env) を編集 (赤字：編集箇所)

```
root@sevone-nms:~/wifi/wifi-solution-v2.9.0-build-174642 [6.1.0] [15:17:17] $ cat /opt/WLCCollector/configuration/cisco.env
SEVONE_API_HOST=127.0.0.1
SEVONE_API_USER=admin
SEVONE_API_PASSWORD=*****(任意のパスワードを記載)
SEVONE_TRANSPORT=api
SEVONE_PERSIST=ram
SEVONE_API_CONFIG_VERSION=v2
SEVONE_API_COLLECTION_VERSION=v2
SEVONE_API_COLLECTION_PORT=80
SEVONE_API_CONFIG_PORT=80
SEVONE_API_SECURITY=False
SEVONE_API_READ_TIMEOUT=60
DEVICE_GROUP=
WLC_VERBOSE=2
WLC_DRY_RUN=
DO_META=True
POLL_INTERVAL=300
TIME_SINCE_AP_UNAVAILABLE=300
WLC_GROUPS=WLC Cisco
DISTRIBUTE_ON_ALL_PEERS=False
DISTRIBUTION_PEERS_LIST=
SELF_MONITORING=True

(省略)
```

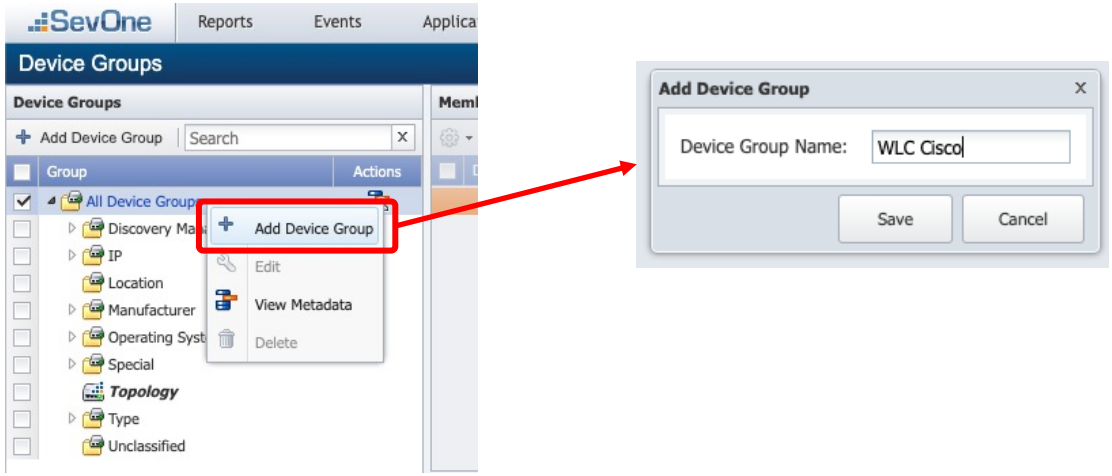

©2022 IBM Corporation

3.5.2.2. WLC Collectorのインストール (4/6)

- Device Group作成
  - 前頁の手順にてcisco.envの「WLC_GROUPS」に指定したDevice Groupを作成する
  - [Devices] > [Grouping] > [Device Groups] を選択



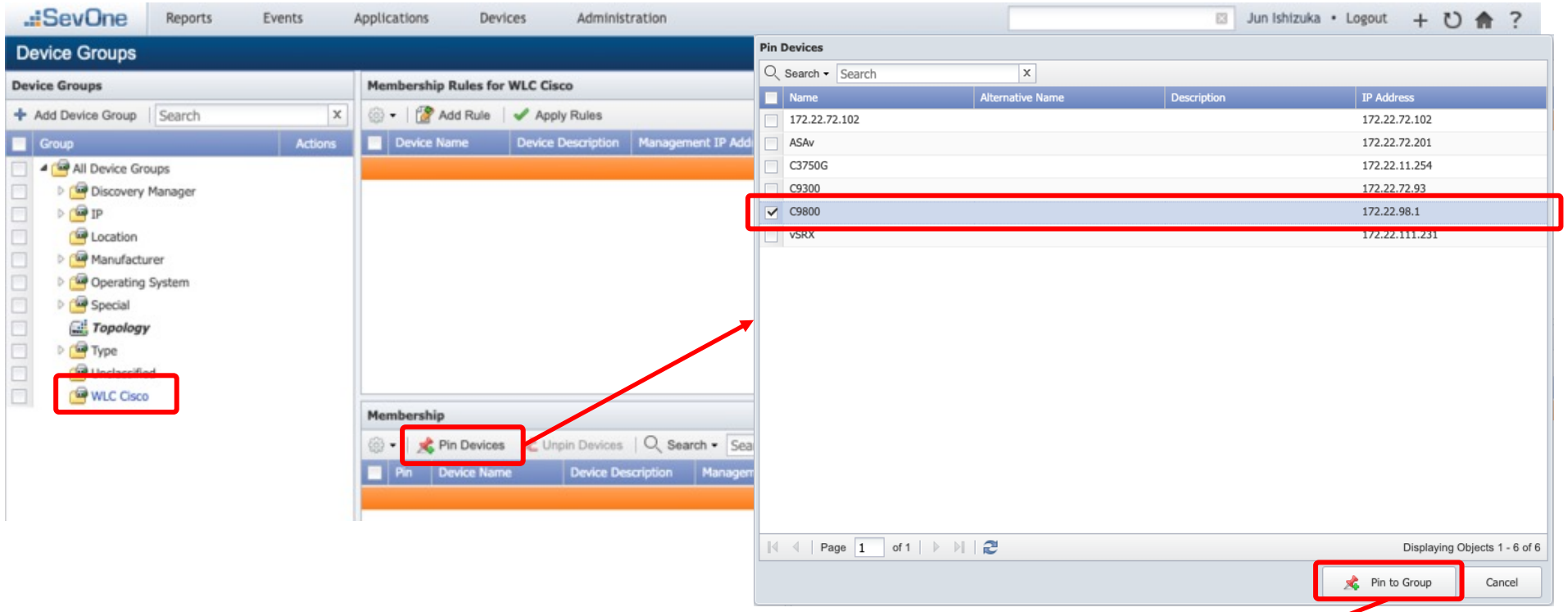
  - [All Device Groups] を右クリック > [Add Device Group] を選択し、「WLC Cisco」を作成

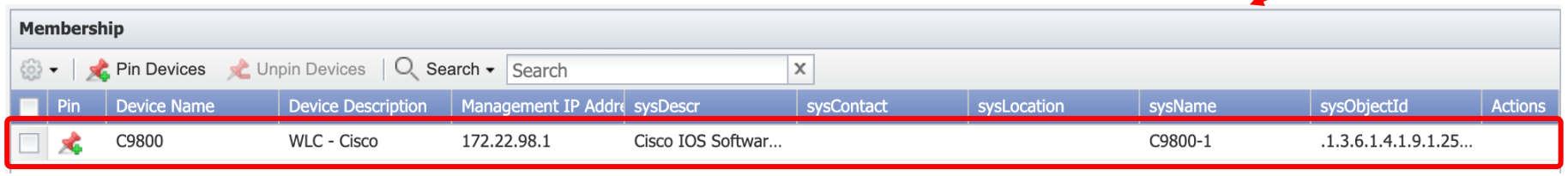


©2022 IBM Corporation

3.5.2.2. WLC Collectorのインストール (5/6)

- 作成したDevice GroupにCisco WLCをPin留め
  - 左メニューより [WLC Cisco] を選択し、[Pin Devices] を選択
  - Device Managerに登録済みのCisco WLC (C9800) にチェックを入れて [Pin to Group] ボタンを押下





©2022 IBM Corporation

3.5.2.2. WLC Collectorのインストール (6/6)

- "./install.sh install" を実行してWLC Collectorをインストール

```
root@sevone-nms:~/wifi/wifi-solution-v2.9.0-build-174642 [6.1.0] [16:58:07] $ ./install.sh install --vendor cisco
OK: User is root.
OK: All the prerequisite requirements met
OK: NMS Version met minimum requirement of 5.7.2.32
OK: Docker version met minimum requirement of 18.06.1 and docker service is up and running.
-----------------------------------------
Installation
-----------------------------------------
OK: Installed cisco-collector
OK: Installation completed successfully
-----------------------------------------
check log file at /var/log/wifi-wlc/wlc_cisco_install.log for any error
root@sevone-nms:~/wifi/wifi-solution-v2.9.0-build-174642 [6.1.0] [16:58:23] $
```


©2022 IBM Corporation

3.5.2.3. WLC Collectorの起動 (1/2)

- "./install.sh run" を実行してWLC Collectorを起動

```
root@sevone-nms:~/wifi/wifi-solution-v2.9.0-build-174642 [6.1.0] [17:00:12] $ ./install.sh run --vendor cisco
OK: User is root.
OK: All the prerequisite requirements met
OK: NMS Version met minimum requirement of 5.7.2.32
OK: Docker version met minimum requirement of 18.06.1 and docker service is up and running.
-------------------------------------------
Running
-------------------------------------------
OK: Cron_file created successfully at /etc/cron.d
OK: logrotate rules files created successfully.
OK: Run completed successfully
-------------------------------------------
check log file at /var/log/wifi-wlc/wlc_cisco_*.log for any error
root@sevone-nms:~/wifi/wifi-solution-v2.9.0-build-174642 [6.1.0] [17:00:17] $
```

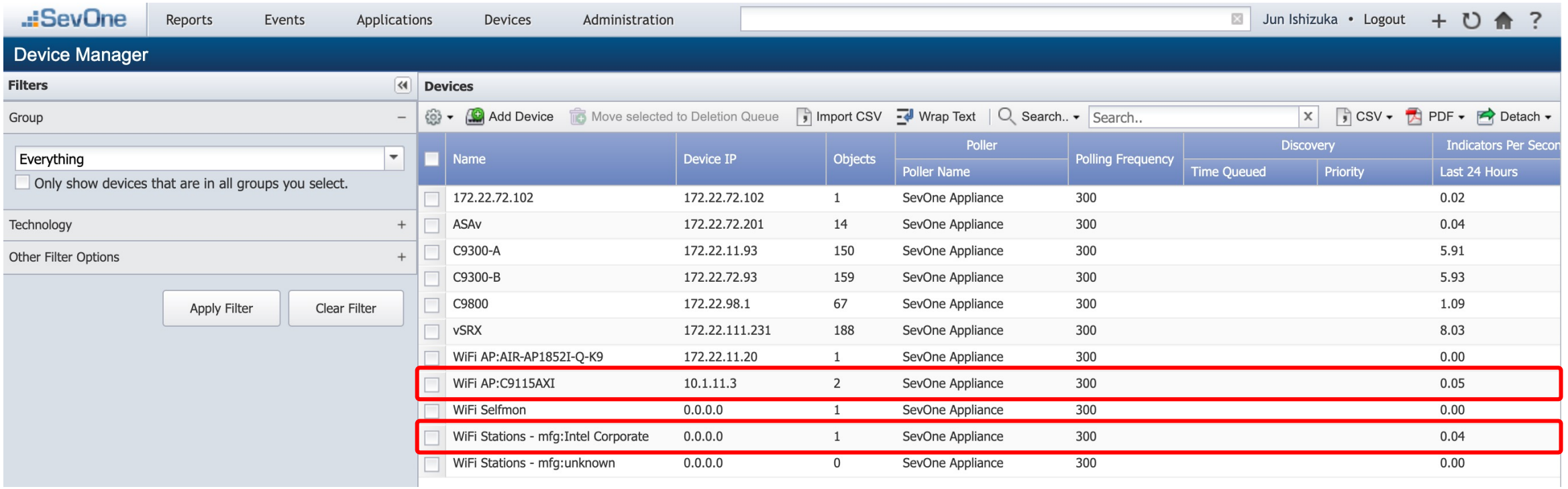
– 正常起動するとcronファイルが生成される

```
root@sevone-nms:~/wifi/wifi-solution-v2.9.0-build-174642 [6.1.0] [09:31:49] $ cat /etc/cron.d/wifi-cron-cisco
# Adding vendor's cronjob
0-59/5 * * * * root [[ $(cat /SevOne.masterslave.master) -ne '0' ]] && /opt/WLCCollector/wlccmd.sh v2.9.0-build-174642 run cisco
```


©2022 IBM Corporation

3.5.2.3. WLC Collectorの起動 (2/2)

- WLC Collectorを起動してしばらくすると、Device ManagerにCisco WLCが管理するAccess Point (AP) およびAPに接続している端末が自動登録される



©2022 IBM Corporation

3.5.3. Wi-Fi widgetsのセットアップ (1/5)

- SDIにSSHログインし、イメージ・ファイルを解凍する

```
[sevone@sevonek8s wifi]$ ls -la
合計 8320
drwxrwxr-x  2 sevone sevone    107  3月 14 18:17 .
drwx------. 6 sevone sevone    151  3月 14 18:17 ..
-rw-r--r--  1 sevone sevone     65  3月 14 18:17 wifi-sdi-widgets-2.9.0-build-174977.sha256.txt
-rw-r--r--  1 sevone sevone 8512512  3月 14 18:17 wifi-sdi-widgets-2.9.0-build-174977.tar


[sevone@sevonek8s wifi]$ tar xvf wifi-sdi-widgets-2.9.0-build-174977.tar
./WifiSolution-ootb-reports-SDI.tar
./ap-audit-table-2.9.0.tgz
./ap-details-2.9.0.tgz
./cisco-ap-inspector-2.9.0.tgz
./cisco-cdp-neighbors-2.9.0.tgz
./delete-widget.sh
./deploy.sh
./heatmap-calendar-1.9.0.tgz
./install-widget.sh
./install.sh
./topn-heatmap-1.9.0.tgz
./version.txt
./wifi-signal-quality-2.9.0.tgz
./wifi-station-details-2.9.0.tgz
./wifi-station-summary-2.9.0.tgz
[sevone@sevonek8s wifi]$
```


©2022 IBM Corporation

3.5.3. Wi-Fi widgetsのセットアップ (2/5)

- "./install.sh" を実行してWi-Fi widget一式をインストール

```
[sevone@sevonek8s wifi]$ ./install.sh wifi-sdi-widgets-2.9.0-build-174977.tar


Verifying installer checksum...
CHECKSUM verified.
Username (the same you use to login to DI): admin
Password (the same you use to login to DI):
Tenant (visible in the bottom left corner below the username, after login): SevOne
DI IP or hostname (no http://; leave blank for: 'sevonek8s'): 172.22.160.54


Attempting to upload: "ap-audit-table-2.9.0.tgz"...
Successful login
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  759k  100     2  100  759k     4  1575k --:--:-- --:--:-- --:--:-- 1574k
Finished uploading.
Attempting to upload: "ap-details-2.9.0.tgz"...
Successful login
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  693k  100     2  100  693k     5  1809k --:--:-- --:--:-- --:--:-- 1807k
Finished uploading.
Attempting to upload: "cisco-ap-inspector-2.9.0.tgz"...
Successful login
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  588k  100     2  100  588k     4  1378k --:--:-- --:--:-- --:--:-- 1380k
Finished uploading.

(次ページへ続く)
```


©2022 IBM Corporation

3.5.3. Wi-Fi widgetsのセットアップ (3/5)

- "./install.sh" を実行してWi-Fi widget一式をインストール

```
(前ページから続き)

Attempting to upload: "cisco-cdp-neighbors-2.9.0.tgz"...
Successful login
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  754k  100    2  100  754k    5  2011k --:--:-- --:--:-- --:--:-- 2018k
Finished uploading.
Attempting to upload: "heatmap-calendar-1.9.0.tgz"...
Successful login
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  862k  100    2  100  862k    5  2510k --:--:-- --:--:-- --:--:-- 2513k
Finished uploading.
Attempting to upload: "topn-heatmap-1.9.0.tgz"...
Successful login
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  867k  100    2  100  867k    5  2371k --:--:-- --:--:-- --:--:-- 2377k
Finished uploading.
Attempting to upload: "wifi-signal-quality-2.9.0.tgz"...
Successful login
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  773k  100    2  100  773k    5  2153k --:--:-- --:--:-- --:--:-- 2159k
Finished uploading.

(次ページへ続く)
```


©2022 IBM Corporation

3.5.3. Wi-Fi widgetsのセットアップ (4/5)

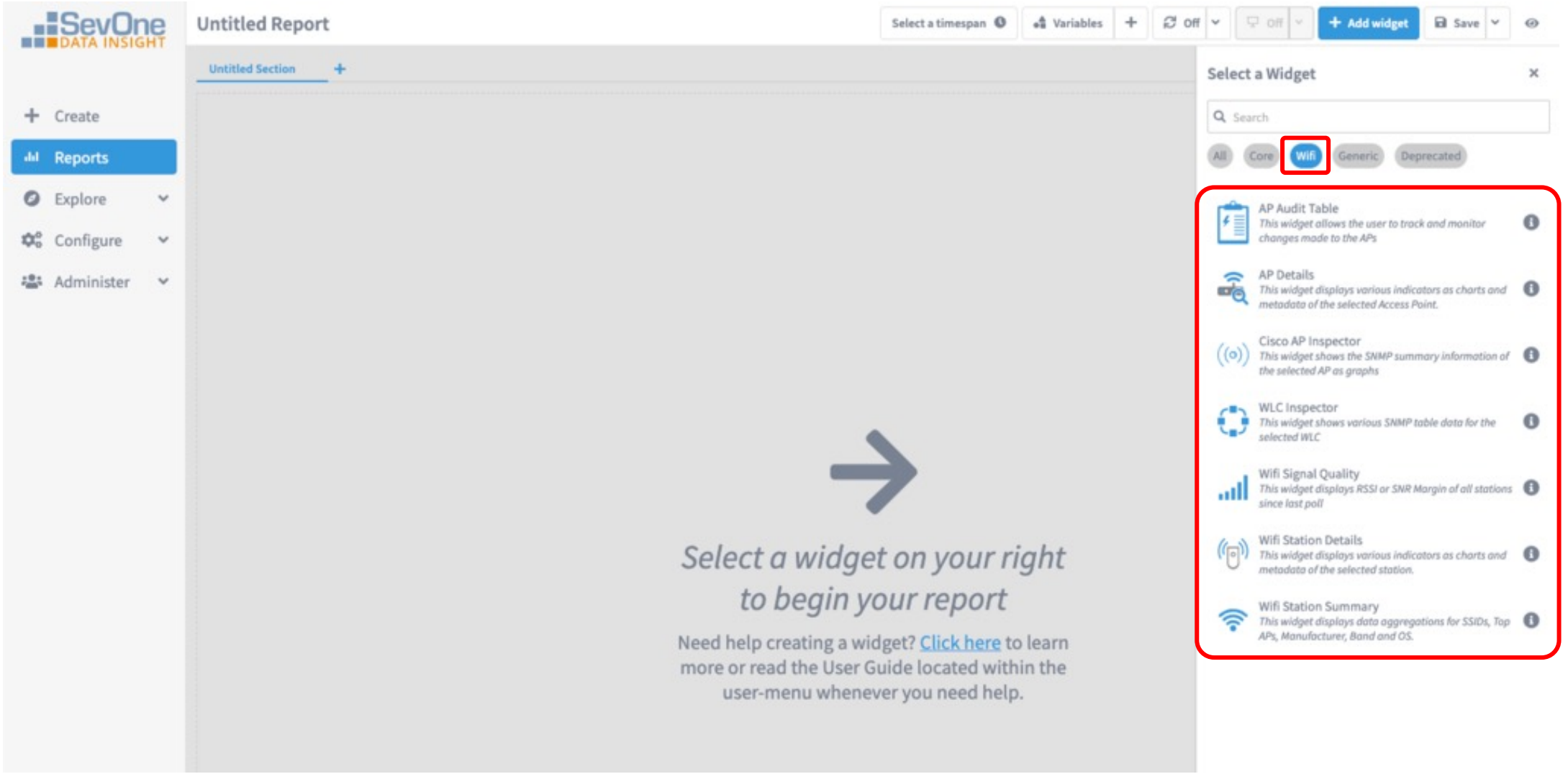
- "./install.sh" を実行してWi-Fi widget一式をインストール

```
(前ページから続き)

Attempting to upload: "wifi-station-details-2.9.0.tgz"...
Successful login
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  694k  100    2  100  694k    6  2124k --:--:-- --:--:-- --:--:-- 2123k
Finished uploading.
Attempting to upload: "wifi-station-summary-2.9.0.tgz"...
Successful login
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100  780k  100    2  100  780k    6  2378k --:--:-- --:--:-- --:--:-- 2373k
Finished uploading.


Installation completed.
[sevone@sevonek8s wifi]$
```


©2022 IBM Corporation

3.5.3. Wi-Fi widgetsのセットアップ (5/5)

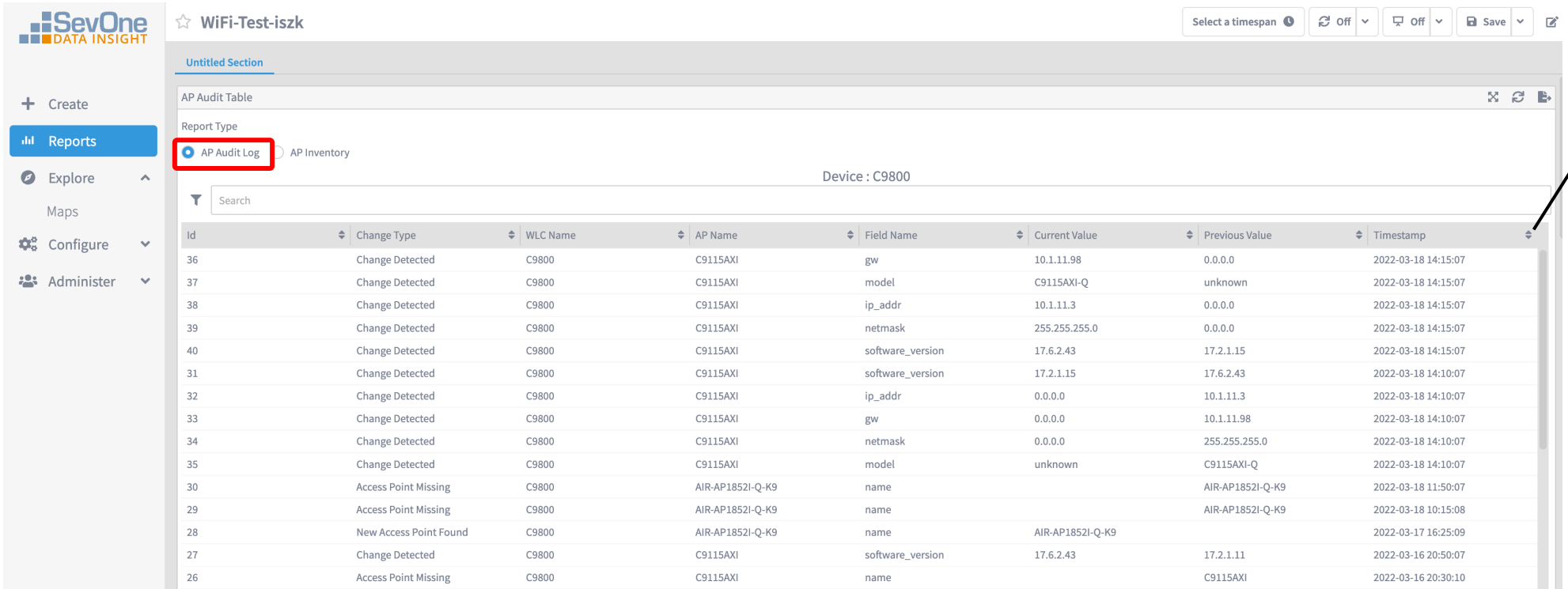
■ インストールが成功すると、Data Insight上にWi-Fi widgetが追加される



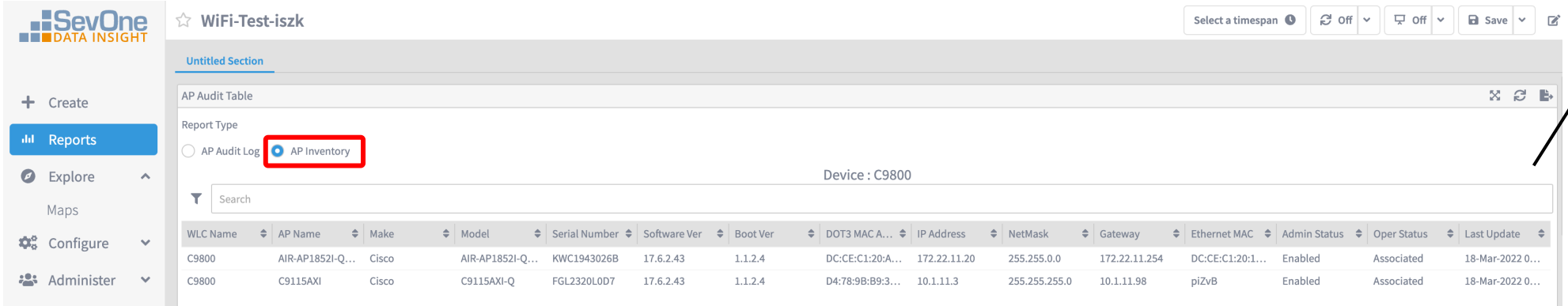
©2022 IBM Corporation

3.5.4. Wi-Fiモニタリング (1/7)

■ AP Audit Table



APのAuditログの確認・検索が可能



APのインベントリー情報の一覧表示が可能

©2022 IBM Corporation

3.5.4. Wi-Fiモニタリング (2/7)

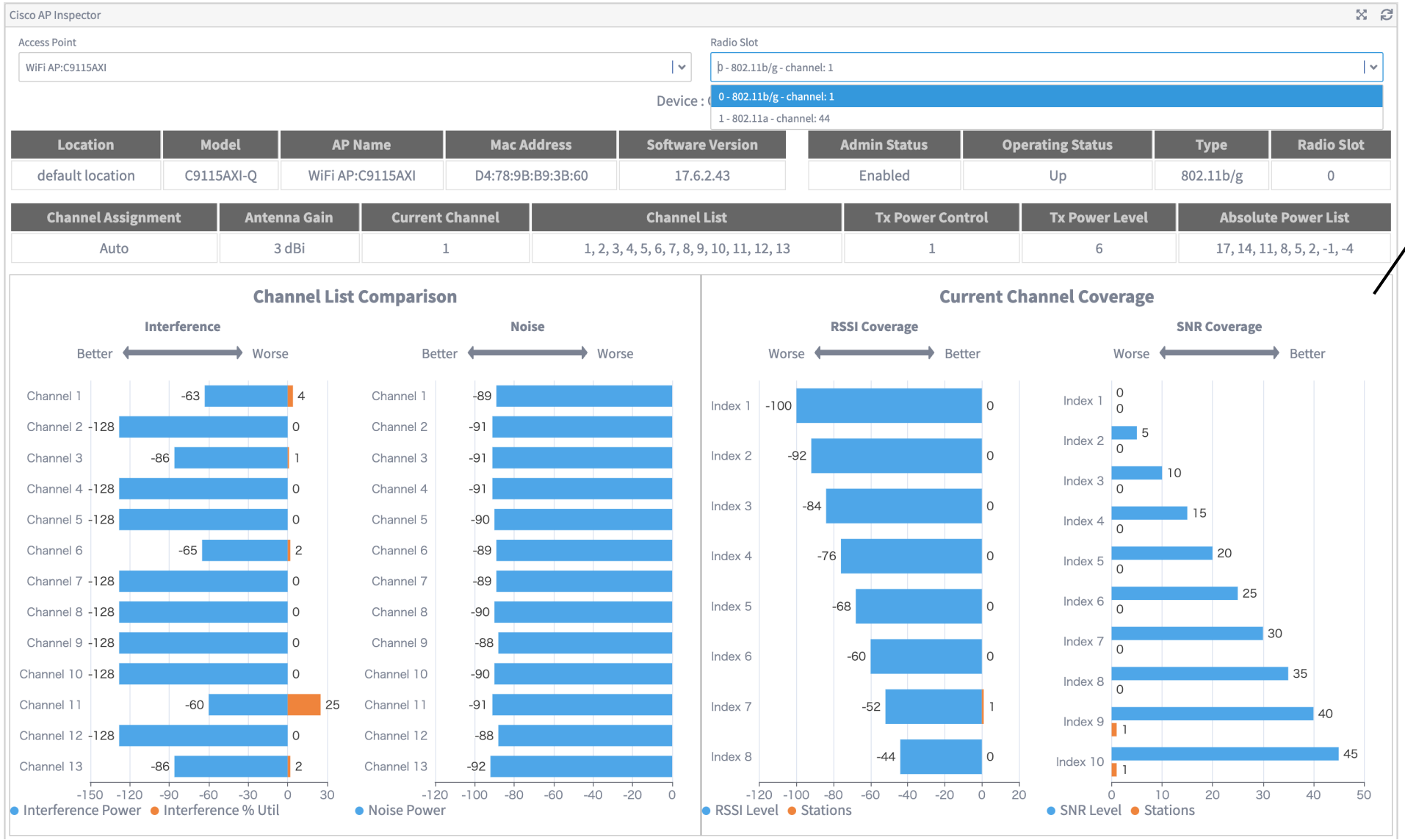
■ AP Details

APの詳細情報 (送受信レート、電波品質、電波強度、ノイズ、接続クライアント数など) を確認可能

©2022 IBM Corporation

3.5.4. Wi-Fiモニタリング (3/7)

■ Cisco AP Inspector

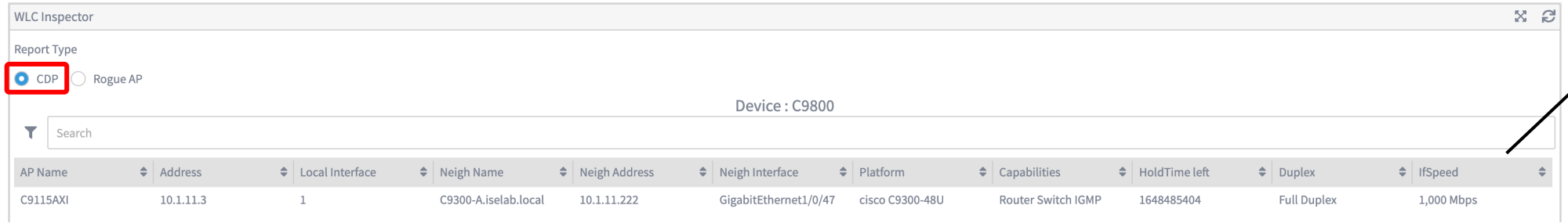


2.4GHz帯/5GHz帯毎に各チャネルの干渉とノイズ状況、現在のチャネルのカバレッジを確認可能

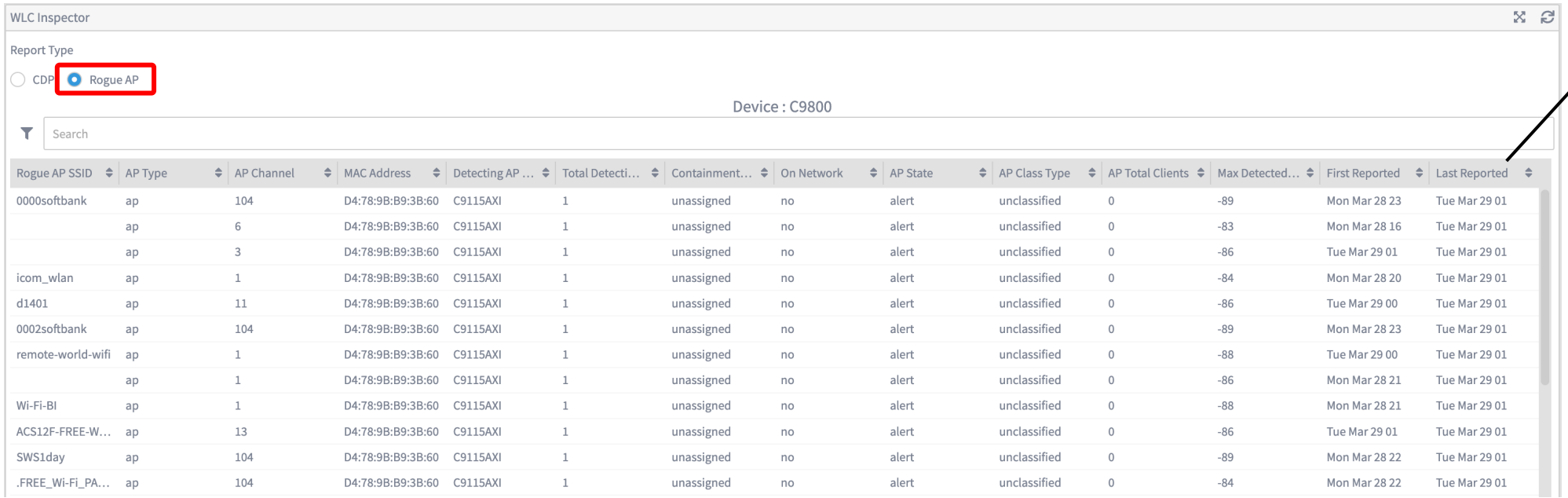
©2022 IBM Corporation

3.5.4. Wi-Fiモニタリング (4/7)

■ WLC Inspector



WLCが管理するAPの隣接機器情報などを確認可能



不正AP (WLCの管理外のAP) 情報などを確認可能

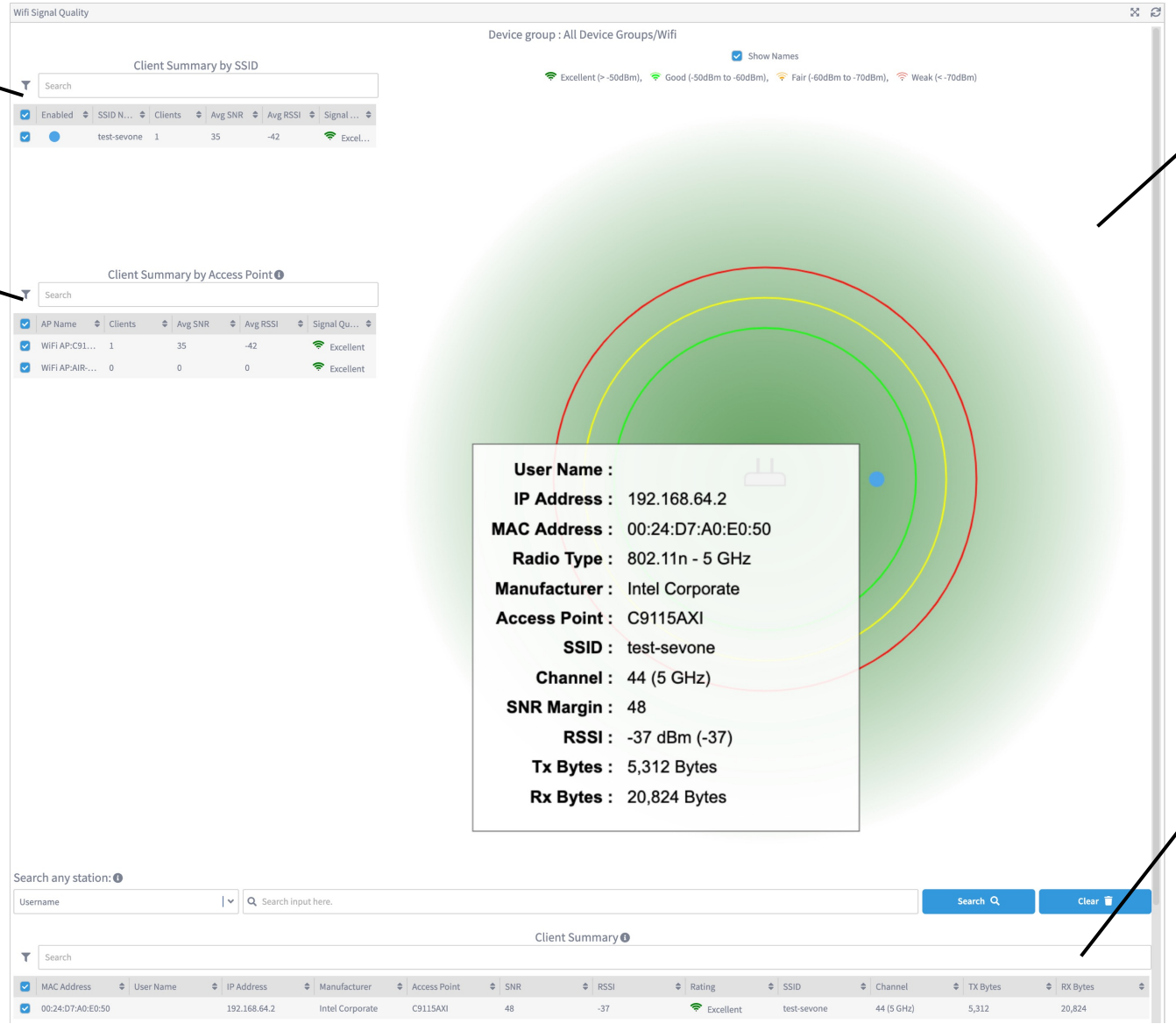
©2022 IBM Corporation

3.5.4. Wi-Fiモニタリング (5/7)

■ Wifi Signal Quality

SSID毎の接続端末数や電波状況

AP毎の接続端末数や電波状況



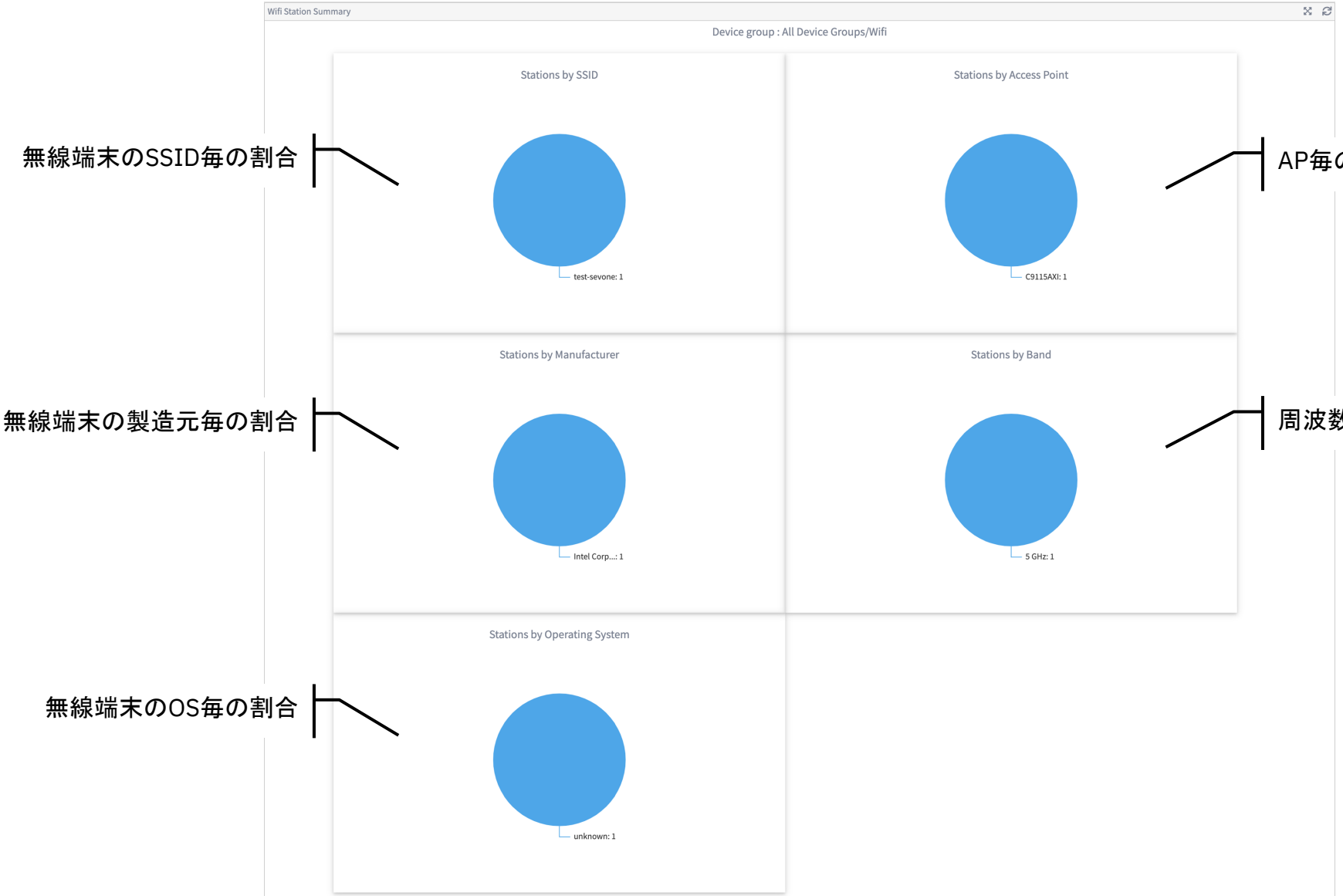
電波品質を視覚的に確認可能

APに接続する無線端末の電波状況などのサマリーを確認可能

©2022 IBM Corporation

3.5.4. Wi-Fiモニタリング (6/7)

■ Wifi Station Summary



無線端末のSSID毎の割合

AP毎の接続端末数の割合

無線端末の製造元毎の割合

周波数帯毎の接続端末数の割合

無線端末のOS毎の割合

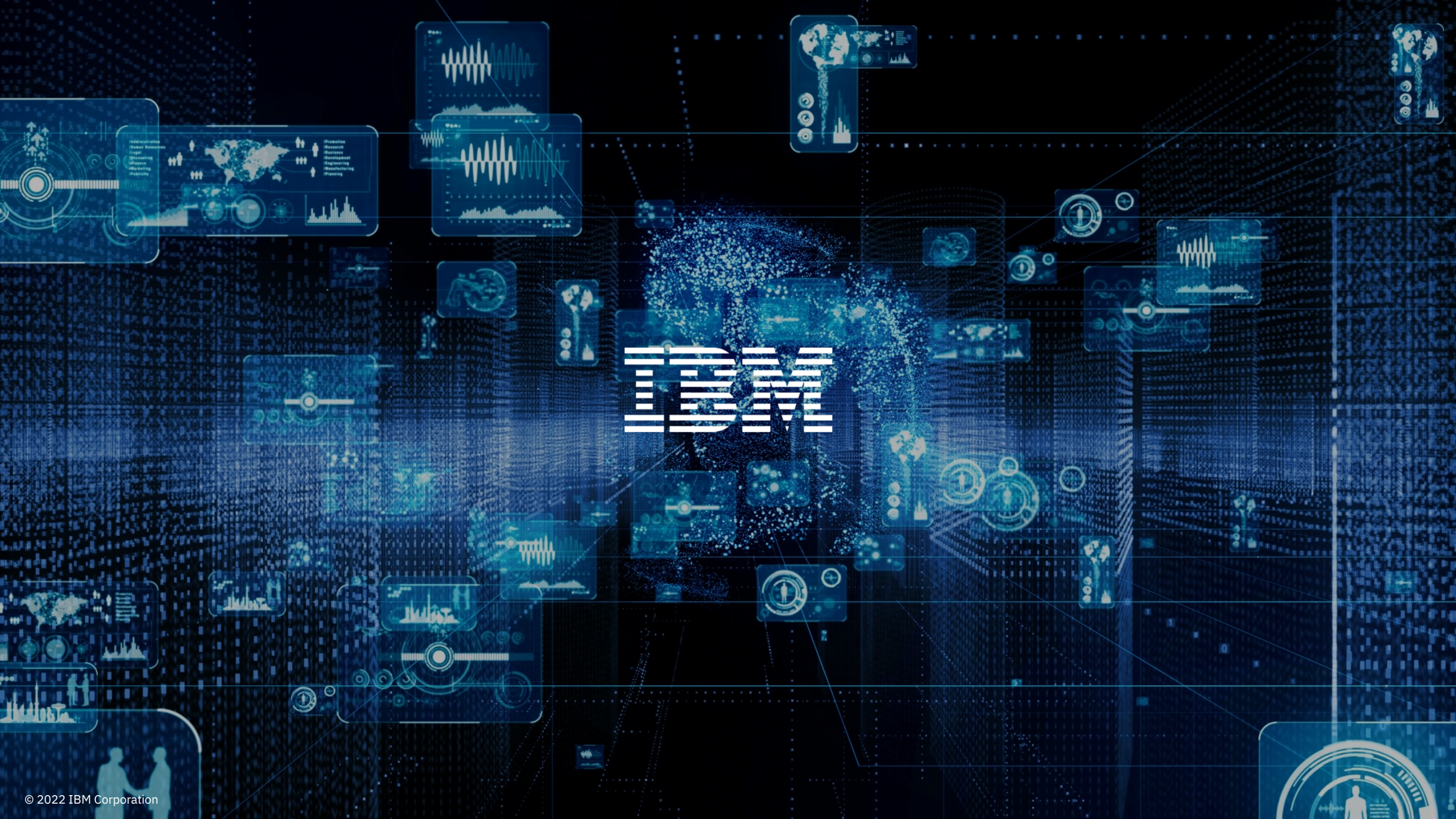
©2022 IBM Corporation

3.5.4. Wi-Fiモニタリング (7/7)

■ Wifi Station Details

無線端末毎の詳細情報(送受信レート、使用周波数帯およびチャネル、電波状況、APとの接続状況など) を確認可能

©2022 IBM Corporation



© 2022 IBM Corporation