|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Benämning | *Kontinuerlig Översyn Kommunikation* | Ansvarig | *Henrik Carlsson* | Skapat | *2015-05-20 09:0939* |
| Projekt |  | | | Senast sparat | *2016-12-23 15:55* |
| Revision | *1.0* | Filnamn | *D-Data Kontinuerlig Översyn Kommunikation.docx* | | |

D-Data Kontinuerlig Översyn Kommunikation

Innehåll

[1 Veckokontroller 5](#_Toc443317231)

[1.1 Switchar / Routrar 5](#_Toc443317232)

[1.1.1 Loggar 5](#_Toc443317233)

[1.2 Brandväggar / VPN (ASA) 5](#_Toc443317234)

[1.2.1 Loggar 5](#_Toc443317235)

[1.3 IPS / URL / AMP (Firepower) 5](#_Toc443317236)

[1.3.1 Patchstatus 5](#_Toc443317237)

[1.3.2 Loggar 5](#_Toc443317238)

[1.4 Trådlöst (WLC/AP) 5](#_Toc443317239)

[1.4.1 Loggar 5](#_Toc443317240)

[1.5 Cisco Security Manager (CSM) 5](#_Toc443317241)

[1.5.1 Loggar 5](#_Toc443317242)

[1.6 FireSight 5](#_Toc443317243)

[1.6.1 Loggar 5](#_Toc443317244)

[1.7 Prime Infrastructure 5](#_Toc443317245)

[1.7.1 Loggar 5](#_Toc443317246)

[1.8 ISE 5](#_Toc443317247)

[1.8.1 Loggar 5](#_Toc443317248)

[2 Halvårskontroller 5](#_Toc443317249)

[2.1 Switchar / Routrar 5](#_Toc443317250)

[2.1.1 Komponentstatus 5](#_Toc443317251)

[2.1.2 Patchstatus 6](#_Toc443317252)

[2.1.3 Supportavtal 6](#_Toc443317253)

[2.1.4 Trendanalys 7](#_Toc443317254)

[2.1.5 Loggar 7](#_Toc443317255)

[2.2 Brandväggar / VPN (ASA) 7](#_Toc443317256)

[2.2.1 Komponentstatus 7](#_Toc443317257)

[2.2.2 Patchstatus 7](#_Toc443317258)

[2.2.3 Supportavtal 7](#_Toc443317259)

[2.2.4 Trendanalys 7](#_Toc443317260)

[2.2.5 Loggar 7](#_Toc443317261)

[2.3 IPS / URL / AMP (Firepower) 7](#_Toc443317262)

[2.3.1 Komponentstatus 7](#_Toc443317263)

[2.3.2 Patchstatus 8](#_Toc443317264)

[2.3.3 Supportavtal 8](#_Toc443317265)

[2.3.4 Trendanalys 8](#_Toc443317266)

[2.3.5 Loggar 8](#_Toc443317267)

[2.4 Trådlöst (WLC/AP) 8](#_Toc443317268)

[2.4.1 Komponentstatus 8](#_Toc443317269)

[2.4.2 Patchstatus 8](#_Toc443317270)

[2.4.3 Supportavtal 8](#_Toc443317271)

[2.4.4 Trendanalys 8](#_Toc443317272)

[2.4.5 Loggar 8](#_Toc443317273)

[2.5 Cisco Security Managet (CSM) 8](#_Toc443317274)

[2.5.1 Komponentstatus 8](#_Toc443317275)

[2.5.2 Patchstatus 9](#_Toc443317276)

[2.5.3 Supportavtal 9](#_Toc443317277)

[2.5.4 Trendanalys 9](#_Toc443317278)

[2.5.5 Loggar 9](#_Toc443317279)

[2.6 FireSight 9](#_Toc443317280)

[2.6.1 Komponentstatus 9](#_Toc443317281)

[2.6.2 Patchstatus 9](#_Toc443317282)

[2.6.3 Supportavtal 9](#_Toc443317283)

[2.6.4 Trendanalys 9](#_Toc443317284)

[2.6.5 Loggar 9](#_Toc443317285)

[2.7 Prime Infrastructure 9](#_Toc443317286)

[2.7.1 Komponentstatus 9](#_Toc443317287)

[2.7.2 Patchstatus 10](#_Toc443317288)

[2.7.3 Supportavtal 10](#_Toc443317289)

[2.7.4 Trendanalys 10](#_Toc443317290)

[2.7.5 Loggar 10](#_Toc443317291)

[2.8 ISE 10](#_Toc443317292)

[2.8.1 Komponentstatus 10](#_Toc443317293)

[2.8.2 Patchstatus 10](#_Toc443317294)

[2.8.3 Supportavtal 10](#_Toc443317295)

[2.8.4 Trendanalys 10](#_Toc443317296)

[2.8.5 Loggar 10](#_Toc443317297)

[3 Summering 10](#_Toc443317298)

[4 Beskrivning av kontroller 11](#_Toc443317299)

[4.1 Switchar / Routrar 11](#_Toc443317300)

[4.2 Brandväggar / VPN (ASA) 11](#_Toc443317301)

[4.3 IPS / URL / AMP (Firepower) 12](#_Toc443317302)

[4.4 Trådlöst (WLC/AP) 13](#_Toc443317303)

[4.5 Cisco Security Manager (CSM) 13](#_Toc443317304)

[4.6 FireSight 14](#_Toc443317305)

[4.7 Prime Infrastructure 15](#_Toc443317306)

[4.8 ISE 15](#_Toc443317307)

# Halvårskontroller

## Switchar / Routrar

### Komponentstatus

**Åtgärd behöver vidtas.**

Det finns 109 switchar och 4 routrar som är ”End of Support” och som starkt rekommenderas att byta ut. Inom 18 månader går ytterligare 22 switchar in i ”End of Support”. En plan för att byta ut dem bör tas fram för att inte hamna i ett läge där det kan bli problem att få support p.g.a. gammal utrustning.

Följande komponenter bör bytas ut:

Router:

2st 2612 EoS 2011-07-31

2st 878 EoS 2016-05-31

Switch:

1st WS-C2912-XL-EN EoS 2006-11-01

3st WS-C2950G-EI EoS 2011-12-31

16st WS-C2950T-24 EoS 2011-12-31

15st WS-C2950-24 EoS 2013-10-31

13st WS-C2950C-24 EoS 2013-10-31

1st WS-C2940-8TF-S EoS 2015-01-31

29st WS-C2940-8TT-S EoS 2015-01-31

6st WS-C3560-24TS-E EoS 2015-07-31

7st WS-C3560-48TS-E EoS 2015-07-31

13st WS-C2960G-24TC-L EoS 2017-07-31

2st WS-C2960G-48TC-L EoS 2017-07-31

1st WS-C2960G-8TC-L EoS 2017-07-31

2st WS-C6513 EoS 2017-08-31

På väg

1st WS-C3560G-48TS-E EoS 2018-01-31

6st WS-C3750G-12S-S EoS 2018-01-31

15st WS-C2960-8TC-L EoS 2018-07-31

För fullständig ”End of Support” rapport se ” 2016-12-05\_consolidated\_report.xls” flik ”Device List (Hardware - EOL)”

### Patchstatus

**Åtgärd behöver vidtas.**

I princip hela switch och router plattformen behöver uppgraderas. Den primära anledningen är att det har upptäckts säkerhetshål i många av mjukvarorna som används idag. Vissa komponenter har släpat uppgraderingsmässigt och ligger långt efter dagens rekommenderade versioner vilket inte är bra vid ex öppnande av supportärenden. Ytterligare en anledning till att uppgradera är att få tillgång till nya funktioner.

Följande komponenter behöver uppgraderas:

* N7K-C7010 CORE 6.2(10) -> 6.2(16)
* Nexus 5500 CORE 5.X.X.X -> 7.2(1)N1(1)
* Nexus 5600 CORE 7.2(1)N1(1)\* -> Ligger på rekommenderad version
* Catalyst 6500 DIST 12.2(33)SXH -> 12.2.33 SXI14
* Catalyst 6800-XL DIST 15.1 -> 15.4.1 SY1
* Catalyst 2960 ACCESS -> uppgraderas till senast rekommenderade mjukvara
* Catalyst 3560 ACCESS -> uppgraderas till senast rekommenderade mjukvara
* Catalyst 3750 ACCESS -> uppgraderas till senast rekommenderade mjukvara
* ISR 878-K9 12.4(4)T7 -> 15.1.4M10

\*Ser ut som en av Nexus 5600 switcharna (n5k4n11) inte ligger på samma version som övriga Nexus 5600 switchar.

För fullständig rapport hur många säkerhetshål det finns i respektive mjukvara se ” 2016-12-05\_consolidated\_report.xls” flik ”Device List (All Devices)”

### Supportavtal

**Ingen åtgärd behöver vidtas.**

Merparten av serviceavtalen på hårdvaran är tecknad med annan leverantör och inte tillgänglig för ATEA. Rekommendationen är att ha full support (hw/sw) på allt som rör datacentret och distributions lagret. På accesslagret räcker det att ha mjukvarusupport för att kunna uppgradera switchar och lägga supportärenden. Vid hårdvarufel är lämpligt att ha reservswitchar på hyllan för snabbt kunna byta trasig enhet.

### Trendanalys

**Ingen åtgärd behöver vidtas.**

Detta kontrollerades inte i nuläget då kund nyttjar snmpc för övervakning av komm-enheter. Vid nästa kontinuerliga översyn kan exempelvis Cisco Prime användas för att ta fram grafer över belastning på länkar & utrustning (förutsatt att utrustning är inlagd som det önskas grafer för).

### Loggar

**Ingen åtgärd behöver vidtas.**

Inget som gjordes inom ramen för detta uppdrag.

# Summering

Det stora jobbet som behöver göras är att uppgradera befintlig kommunikationsutrustning så att den kommer upp i rekommenderad och enhetlig nivå. Uppgraderingarna har släpat en del och omtag behöver göras för att komma i fas. Det finns även en hel del switchar och routrar som behöver bytas ut pga att de har gått eller kommer att gå ”End of Support” i närtid. I det stora hela har Landstinget ett väl fungerade nät men det kräver kontinuerligt underhåll för att fungera så optimalt som möjligt.

# Beskrivning av kontroller

## Switchar / Routrar

|  |  |  |
| --- | --- | --- |
| **Funktion** | **Kontroll** | **Verktyg** |
| Switching / Routing | **Komponentstatus**, kontrollera End-of-Life, End-of-Sale, End of SW Maintenance, End of Service Contract Renewal, Lats Day of Support. | Cisco Active Advisor (rapport) |
| Switching / Routing | **Patchstatus**, kontrollera om nuvarande version har några kritiska buggar, ge förslag på nästkommande stabila version som är lämplig att uppgradera till för att inte släpa efter för mycket. | Cisco Active Advisor (rapport) + manuellt arbete som infogas som kommentarer till rapporten |
| Switching / Routing | **Supportavtal**, kontrollera att giltiga avtal finns på kritiska komponenter och ge förslag vad som bör läggas till alt tas bort. | Cisco Active Advisor (rapport) |
| Switching / Routing | **Trendanalys**, kontrollera CPU, flash och minnesutnyttjande samt bandbreddsutnyttjande på kritiska länkar. | Cisco Prime Infrastructure (rapport) |
| Switching / Routing | **Loggar**  Veckokontroll, sammanställa alla meddelande i alarmloggen sen senaste veckkontrollen och kommentera nya händelser + eventuella åtgärder som bör vidtas.  Halvårskontroll, sammanställa alla händelser sen senaste halvårskontrollen + veckokontroller och kommentera händelser och trender + eventuella åtgärder som bör vidtas. |  |