

SOCECAP Orléans

Audit LAN

HCS/AST

CHOUARHI Yacine

Sommaire

[1 - Introduction 4](#_Toc447072)

[1.1 Définition du périmètre de l’audit 4](#_Toc447073)

[1.2 Executive summary 7](#_Toc447074)

[1.3 Structure du document 8](#_Toc447075)

[1.4 Revision du document 8](#_Toc447076)

[2 - Administration 9](#_Toc447077)

[2. Schéma physique du réseau Sogecap Orléans 9](#_Toc447078)

[2.1 Inventaire opérationnel 10](#_Toc447079)

[2.1 Monitoring des équipements 12](#_Toc447080)

[2.2 Gestion des syslogs 12](#_Toc447081)

[2.1 NTP 13](#_Toc447082)

[3 - Sécurité des équipements 15](#_Toc447083)

[3.1 SNMP 15](#_Toc447084)

[3.2 Accès ACL des équipements 15](#_Toc447085)

[3.3 Serveurs HTTP / HTTPS 17](#_Toc447086)

[3.4 Configuration Radius 17](#_Toc447087)

[3.5 Utilisateurs locaux 17](#_Toc447088)

[4 - Layer 2 18](#_Toc447089)

[4.1 VTP 18](#_Toc447090)

[4.2 Mode Spanning-tree 19](#_Toc447091)

[4.3 Domaine Spanning-tree 19](#_Toc447092)

[4.4 Topologie Spanning-tree 20](#_Toc447093)

[4.5 Customisation spanning-tree 21](#_Toc447094)

[4.6 CDP 21](#_Toc447095)

[4.7 UDLD 22](#_Toc447096)

[4.8 Storm-control 22](#_Toc447097)

[4.9 DHCP snooping 22](#_Toc447098)

[4.10 ARP inspection 23](#_Toc447099)

[4.11 IGMP snooping 23](#_Toc447100)

[4.12 MTU 23](#_Toc447101)

[4.13 Etherchannel 23](#_Toc447102)

[5 - Layer 3 24](#_Toc447103)

[5.1 Routage Statique 24](#_Toc447104)

[5.2 Routage Dynamique 25](#_Toc447105)

[5.2.1 OSPF 25](#_Toc447106)

[5.3 BGP 28](#_Toc447107)

[5.4 HSRP 30](#_Toc447108)

[6 - Performance 34](#_Toc447109)

[6.1 Utilisation mémoire et CPU 34](#_Toc447110)

[6.2 Utilisation TCAM 34](#_Toc447111)

[6.3 Erreurs sur les interfaces 35](#_Toc447112)

[7 - Best Practice 36](#_Toc447113)

[7.1 VSS 36](#_Toc447114)

[7.2 HSRP 36](#_Toc447115)

[7.2.1 HSRP Authentification 36](#_Toc447116)

[7.2.1 Standby Delay Minimum Reload 37](#_Toc447117)

[7.1 Mac adresse Move 37](#_Toc447118)

# Introduction

À la suite des différents incidents survenus dans l’infra LAN-DC Orléans, il a été recommandé de faire un audit datacenter des sites Sogecap Orléans, il a pour but de mettre en avant les éventuelles faiblesses de conception, de matériel et de configuration des éléments qui composent l’infrastructure réseau.

L’objectif final est l’amélioration de la stabilité et de la performance du réseau Sogecap Orléans.

## Définition du périmètre de l’audit

Le réseau Sogecap Orléans est composé de deux sites : Alexandrin et Campus.

Le périmètre de l’audit prend en compte l’ensemble des équipements de :

* cœurs / distribution
* Routeur WAN ( interconnexion avec le MAN SG )

L’inventaire Réseau fournit par Sogecap est le suivant :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SITE** | **NOM** | **MARQUE** | **MODELE** | **IP** | **VERSION** |
| ALEXANDRIN | OCCORE-VSS | CISCO | WS-C6506-E | 10.45.140.253 | 15.1(2)SY10 |
| ALEXANDRIN | CISCO | WS-C6506-E | 15.1(2)SY10 |
| ALEXANDRIN | OCN5K01 | CISCO | NEXUS 5548UP | 192.116.34.39 | 7.1(4)N1(1) |
| ALEXANDRIN | OCN5K02 | CISCO | NEXUS 5548UP | 192.116.34.38 | 7.1(4)N1(1) |
| ALEXANDRIN | OCN5K03 | CISCO | NEXUS 5548UP | 192.116.34.37 | 7.1(4)N1(1) |
| ALEXANDRIN | OCN5K04 | CISCO | NEXUS 5548UP | 192.116.34.36 | 7.1(4)N1(1) |
| ALEXANDRIN | OCN5K05 | CISCO | NEXUS 5548UP | 192.116.34.25 | 7.1(4)N1(1) |
| ALEXANDRIN | OCN5K06 | CISCO | NEXUS 5548UP | 192.116.34.24 | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KE91 | CISCO | NEXUS 2248TP |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KE92 | CISCO | NEXUS 2248TP |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KS93 | CISCO | NEXUS 2248TP |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB01 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB02 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB11 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB12 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB21 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB22 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB31 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB32 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB41 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB42 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB51 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB52 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB61 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB62 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB71 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB72 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB181 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB182 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB191 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB192 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB201 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN2KB202 | CISCO | NEXUS 2248TP-E |  | 7.1(4)N1(1) |
| ALEXANDRIN | OCN3KSAS1 | CISCO | NEXUS 3064-T | 192.116.34.32 | 6.0(2)U2(2) |
| ALEXANDRIN | OCN3KSAS2 | CISCO | NEXUS 3064-T | 192.116.34.33 | 6.0(2)U2(2) |
| ALEXANDRIN | OCN3KBIG1 | CISCO | NEXUS 3064-T | 190.116.34.73 | 6.0(2)U3(7) |
| ALEXANDRIN | OCN3KBIG2 | CISCO | NEXUS 3064-T | 190.116.34.74 | 6.0(2)U3(7) |
| ALEXANDRIN | OCCISSAN01 | CISCO | 2960G-24TC-L | 192.116.34.40 | 15.0(2)SE5 |
| ALEXANDRIN | OCCISCOM01 | CISCO | 2960G-24TC-L | 192.116.34.47 | 15.0(2)SE5 |
| ALEXANDRIN | OCCISMON01 | CISCO | 2960X-24TS-L | 192.116.34.80 | 15.0(2A)EX5 |
| ALEXANDRIN | OCCISDMZ1 | CISCO | 2960X-48TS-L | 192.116.33.137 | 15.2(3)E1 |
| ALEXANDRIN | OCCISDMZ2 | CISCO | 2960X-48TS-L | 192.116.33.138 | 15.2(3)E1 |
| ALEXANDRIN | OCCNET50 | CISCO | 2960X-24TS-L | 192.116.33.149 | 15.0(2a)EX5 |
| ALEXANDRIN | OCLNET50 | RADWARE | OnDemand Switch VL 208 | 10.45.155.36 | lp-6.13.00 |
| ALEXANDRIN | OQPNET50 | BLUECOAT | PackeShaper 12000 | 192.116.33.143 | v9.2.13g1 |
| ALEXANDRIN | OCALTLAN3 | RADWARE | 4408 | 192.116.34.75 | 30.0.5.0 |
| ALEXANDRIN | OCALTDMZ3 | RADWARE | 4408 | 192.116.33.133 | 30.0.5.0 |
| ALEXANDRIN | OCALTLAN20 | RADWARE | 4408 | 192.116.34.41 | 30.0.5.0 |
| ALEXANDRIN | OCALTDMZ20 | RADWARE | 4408 | 192.116.33.135 | 30.0.5.0 |
| ALEXANDRIN | OWCASA50 | CISCO | ASA5525-X | 10.45.140.250 | 9.4(4).5 |
| ALEXANDRIN | ORCWAN1 | CISCO | 3925E | 10.45.156.1 | 15.4(3)M5 |
| ALEXANDRIN | OWNET1 | JUNIPER | netscreen-SSG140 | 192.116.33.145 | 6.3.0r23.0 |
| ALEXANDRIN | OSLSOP50 | Sophos | SM2000 | 192.116.34.72 | 4.3.6 |
| ALEXANDRIN | OSLSOP51 | Sophos | ws1100b | 192.116.14.51 | 4.3.6 |
| ALEXANDRIN | OSACS50 | CISCO | 1121 | 192.116.34.15 | 5.4.0.46.0a |
| ALEXANDRIN | OCCISICO1 | CISCO | 2960XR-48TS-I | 192.116.34.106 | 15.0(2)EX5 |
| ALEXANDRIN | OCCISICO2 | CISCO | 2960XR-48TS-I | 192.116.34.107 | 15.0(2)EX5 |
|  |  |  |  |  |  |
| ALEXANDRIN | OCCISBLDBUR01 | CISCO | CBS-3110G | 192.116.34.19 | 12.2(55)SE5 |
| ALEXANDRIN | OCCISBLDWEB01 | CISCO | CBS-3110G | 192.116.34.20 | 12.2(55)SE5 |
| ALEXANDRIN | OCCISBLDWEB02 | CISCO | CBS-3110G | 192.116.34.22 | 12.2(55)SE5 |
| ALEXANDRIN | OCCISBLDMOS01 | CISCO | CBS-3110X | 192.116.34.21 | 12.2(55)SE5 |
| ALEXANDRIN | OCCISBLDWEB03 | CISCO | CBS-3110G | 192.116.34.23 | 12.2(55)SE5 |
| ALEXANDRIN | OCCISBLDSUR01 | CISCO | CBS-3110X | 192.116.34.24 | 12.2(55)SE5 |
| ALEXANDRIN | OCCISBLDBUR03 | CISCO | CBS-3110G | 192.116.34.17 | 12.2(55)SE5 |
| ALEXANDRIN | OCDELFOR01 | DELL | MXL-10/40GbE | 192.116.34.101 | 9.10(0.1P19) |
| ALEXANDRIN | OCDELFOR02 | DELL | MXL-10/40GbE | 192.116.34.102 | 9.9(0.0) |
| ALEXANDRIN | OCIBMPUR1 | IBM | IBM Flex System EN2092 1Gb Ethernet Scalable Switch | 192.116.17.134 | 7.2.6.0 |
| ALEXANDRIN | OCIBMPUR2 | IBM | IBM Flex System EN2092 1Gb Ethernet Scalable Switch | 192.116.17.135 | 7.2.6.0 |
| ALEXANDRIN | OCIBMPUR5 | IBM | IBM Flex System EN2092 1Gb Ethernet Scalable Switch | 192.116.17.138 | 7.2.6.0 |
| ALEXANDRIN | OCIBMPUR6 | IBM | IBM Flex System EN2092 1Gb Ethernet Scalable Switch | 192.116.17.139 | 7.2.6.0 |
| ALEXANDRIN | OCIBMPUR9 | IBM | IBM Flex System EN2092 1Gb Ethernet Scalable Switch | 192.116.34.68 | 7.7.5 |
| ALEXANDRIN | OCIBMPUR10 | IBM | IBM Flex System EN2092 1Gb Ethernet Scalable Switch | 192.116.34.69 | 7.7.5 |
| ALEXANDRIN | OCIBMPUR13 | IBM | IBM Flex System EN4093 10Gb Ethernet Scalable Switch | 192.116.17.72 | 7.8.8 |
| ALEXANDRIN | OCIBMPUR14 | IBM | IBM Flex System EN4093 10Gb Ethernet Scalable Switch | 192.116.17.73 | 7.8.8 |
| ALEXANDRIN | OCIBMPUR17 | IBM | IBM Flex System EN4093 10Gb Ethernet Scalable Switch | 192.116.34.66 | 7.8.8 |
| ALEXANDRIN | OCIBMPUR19 | IBM | IBM Flex System EN4093 10Gb Ethernet Scalable Switch | 192.116.34.85 192.116.34.86 | 7.8.8 |
| ALEXANDRIN | ONC3KNDG1 | CISCO | NEXUS 3172PQ-XL | 192.116.34.71 | 7.0(3)I5(1) |
| ALEXANDRIN | OCN2KB251 | CISCO | N2K-C2248TP-E-1GE V03 |  |  |
| ALEXANDRIN | OCN2KB252 | CISCO | N2K-C2248TP-E-1GE V03 |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **SITE** | **NOM** | **MARQUE** | **MODELE** | **IP** | **VERSION** |
| CAMPUS | DCCISOOB50 | CISCO | WS-C2960X-48TS-L | 192.116.21.4 | 15.2(3)E1 |
| CAMPUS | CISCO | WS-C2960X-48TS-L | 15.2(3)E1 |
| CAMPUS | DCCORE-VSS | CISCO | WS-C6506-E | 192.116.34.3 | 15.1(2)SY10 |
| CAMPUS |  | CISCO | WS-C6506-E |  | 15.1(2)SY10 |
| CAMPUS | DCN5K50 | CISCO | Nexus 5672UP | 192.116.21.6 | 7.1(4)N1(1) |
| CAMPUS | DCN5K51 | CISCO | Nexus 5672UP | 192.116.21.7 | 7.1(4)N1(1) |
| CAMPUS | DCN5K52 | CISCO | Nexus 5672UP | 192.116.21.8 | 7.1(4)N1(1) |
| CAMPUS | DCN5K53 | CISCO | Nexus 5672UP | 192.116.21.9 | 7.1(4)N1(1) |
| CAMPUS | DCCORE3 | CISCO | WS-C6506-E | 192.116.21.1 | 12.2(50r)SYS3 |
| CAMPUS | DCCORE4 | CISCO | WS-C6506-E | 192.116.21.1 | 12.2(50r)SYS3 |
| CAMPUS | DCN2K101 | CISCO | N2K-C2348TQ-10GE |  | 7.1(4)N1(1) |
| CAMPUS | DCN2K102 | CISCO | N2K-C2348TQ-10GE |  | 7.1(4)N1(1) |
| CAMPUS | DCN2K103 | CISCO | N2K-C2348TQ-10GE |  | 7.1(4)N1(1) |
| CAMPUS | DCN2K104 | CISCO | N2K-C2348TQ-10GE |  | 7.1(4)N1(1) |
| CAMPUS | DCN2K105 | CISCO | N2K-C2348TQ-10GE |  | 7.1(4)N1(1) |
| CAMPUS | DCN2K106 | CISCO | N2K-C2348TQ-10GE |  | 7.1(4)N1(1) |
| CAMPUS | DCN2K107 | CISCO | N2K-C2348TQ-10GE |  | 7.1(4)N1(1) |
| CAMPUS | DCN2K108 | CISCO | N2K-C2348TQ-10GE |  | 7.1(4)N1(1) |
| CAMPUS | DCN2K109 | CISCO | N2K-C2348TQ-10GE |  | 7.1(4)N1(1) |
| CAMPUS | DCN2K110 | CISCO | N2K-C2348TQ-10GE |  | 7.1(4)N1(1) |
| CAMPUS | DCCDMZ52 | CISCO | WS-C2960X-24TS-L WS-C2960X-24TS-L | 192.116.33.153 | 15.0(2a)EX5 15.0(2a)EX5 |
| CAMPUS | DCCORE50 | CISCO | NEXUS 3548P-10G | 192.116.34.55 | 6.0(2)A6(7) |
| CAMPUS | DCCORE51 | CISCO | NEXUS 3548P-10G | 192.116.34.56 | 6.0(2)A6(7) |
| CAMPUS | DCN3KSAS3 | CISCO | NEXUS 3064-T | 192.116.34.53 | 6.0(2)U2(2) |
| CAMPUS | DCN3KSAS4 | CISCO | NEXUS 3064-T | 192.116.34.54 | 6.0(2)U2(2) |
| CAMPUS | DCN3KBIG3 | CISCO | NEXUS 3064-T | 192.116.34.92 | 6.0(2)U3(7) |
| CAMPUS | DCN3KBIG4 | CISCO | NEXUS 3064-T | 192.116.34.93 | 6.0(2)U3(7) |
| CAMPUS | DCCISDMZ3 | CISCO | 2960X-48TS-L | 192.116.33.139 | 15.2(3)E1 |
| CAMPUS | DCCISDMZ4 | CISCO | 2960X-48TS-L | 192.116.33.140 | 15.2(3)E1 |
| CAMPUS | DCCNET51 | CISCO | 2960X-24TS-L | 192.116.33.150 | 15.0(2a)EX5 |
| CAMPUS | DCLNET51 | RADWARE | 208 | 192.116.33.148 | lp-6.13.00 |
| CAMPUS | DQPNET51 | BLUECOAT | PackeShaper 12000 | 192.116.33.144 | v9.2.13g1 |
| CAMPUS | DCALTLAN4 | RADWARE | 4408 | 192.116.34.76 | 30.0.5.0 |
| CAMPUS | DCALTDMZ4 | RADWARE | 4408 | 192.116.33.134 | 30.0.5.0 |
| CAMPUS | DCALTLAN20 | RADWARE | 4408 | 192.116.34.43 | 30.0.5.0 |
| CAMPUS | DCALTDMZ20 | RADWARE | 4408 | 192.116.33.136 | 30.0.5.0 |
| CAMPUS | DWCASA51 | CISCO | ASA5525-X | 10.45.140.251 | 9.4(4).5 |
| CAMPUS | DRCWAN2 | CISCO | 3925E | 10.45.156.2 | 15.4(3)M5 |
| CAMPUS | DCCISTOP50 | CISCO | netscreen-SsG140 | 192.116.33.146 | 6.3.0r23.0 |
| CAMPUS | DWNET2 | JUNIPER | ws1100b | 192.116.14.52 | 4.3.6 |
| CAMPUS | DSLSOP52 | Sophos | 1121 | 192.116.34.16 | 5.4.0.46.0a |
| CAMPUS | DSACS51 | CISCO | 2960G-24TC-L | 192.116.34.46 | 15.0(2)SE5 |
| CAMPUS | DCCISSAN02 | CISCO | 2960X-24TS-L | 192.116.34.81 | 15.0(2A)EX5 |
| CAMPUS | DCCISMON02 | CISCO | CBS-3110G | 192.116.34.28 | 12.2(55)SE5 |
| CAMPUS | DCCISBLDBUR01 | CISCO | CBS-3110G | 192.116.34.25 | 12.2(55)SE5 |
| CAMPUS | DCCISBLDBUR02 | CISCO | CBS-3110G | 192.116.34.27 | 12.2(55)SE5 |
| CAMPUS | DCCISBLDWEB01 | CISCO | CBS-3110G | 192.116.34.29 | 12.2(55)SE5 |
| CAMPUS | DCCISBLDMOS01 | CISCO | CBS-3110G | 192.116.34.26 | 12.2(55)SE5 |
| CAMPUS | DCCISBLDMOS02 | CISCO | CBS-3110G | 192.116.34.30 | 12.2(55)SE5 |
| CAMPUS | DCCISBLDSUR01 | CISCO | CBS-3110G | 192.116.34.31 | 12.2(55)SE5 |
| CAMPUS | DCCISBLDSUR02 | CISCO | MXL-10/40GbE | 192.116.34.97 | 9.10(0.1P19) |
| CAMPUS | DCDELFOR03 | DELL | MXL-10/40GbE | 192.116.34.98 | 9.10(0.1P19) |
| CAMPUS | DCDELFOR04 | DELL | MXL-10/40GbE | 192.116.34.99 | 9.10(0.1) |
| CAMPUS | DCDELFOR05 | DELL | MXL-10/40GbE | 192.116.34.103 | 9.10(0.1) |
| CAMPUS | DCDELFOR06 | DELL | IBM Flex System EN2092 1Gb Ethernet Scalable Switch | 192.116.17.131 | 7.2.6.0 |
| CAMPUS | DCIBMPUR3 | IBM | IBM Flex System EN2092 1Gb Ethernet Scalable Switch | 192.116.17.132 | 7.2.6.0 |
| CAMPUS | DCIBMPUR4 | IBM | IBM Flex System EN2092 1Gb Ethernet Scalable Switch | 192.116.17.126 | 7.2.6.0 |
| CAMPUS | DCIBMPUR7 | IBM | IBM Flex System EN2092 1Gb Ethernet Scalable Switch | 192.116.17.127 | 7.2.6.0 |
| CAMPUS | DCIBMPUR8 | IBM | IBM Flex System EN2092 1Gb Ethernet Scalable Switch | 192.116.34.57 | 7.7.5 |
| CAMPUS | DCIBMPUR11 | IBM | IBM Flex System EN4093 10Gb Ethernet Scalable Switch | 192.116.17.78 | 7.8.5 |
| CAMPUS | DCIBMPUR15 | IBM | IBM Flex System EN4093 10Gb Ethernet Scalable Switch | 192.116.17.79 | 7.8.5 |
| CAMPUS | DCIBMPUR16 | IBM | IBM Flex System EN4093 10Gb Ethernet Scalable Switch | 192.116.34.67 | 7.8.8 |
| CAMPUS | DCIBMPUR18 | IBM | IBM Flex System EN4093 10Gb Ethernet Scalable Switch | 192.116.34.82 192.116.34.83 | 7.8.8 |
| CAMPUS | DCIBMPUR20 | IBM | Cisco Nexus N3K-C3172PQ-XL | 192.116.21.50 | ? |
| CAMPUS | DCN3K50 | CISCO | Cisco Nexus N3K-C3172PQ-XL | 192.116.21.51 | ? |
| CAMPUS | DCN3K51 | CISCO | Cisco Nexus N3K-C3172PQ-XL | 192.116.21.52 | ? |
| CAMPUS | DCN3K52 | CISCO | Cisco Nexus N3K-C3172PQ-XL | 192.116.21.53 | ? |
| CAMPUS | DCN3K53 | CISCO |  |  |  |

## Executive summary

Le réseau Sogecap est constitué de deux sites (Campus et Alexandrin), ces deux sites sont interconnectés via un cœur de réseau constitué de deux switchs Cisco 6500 en VSS (virtual-switching-system) sur le site Alexandrin (OCCORE-VSS) et un autre VSS sur le site Campus (DCCORE-VSS-2).

Deux liaisons 10G interconnectent les deux sites de manière redondante l’une de l’autre.

L’ensemble du routage (Default Gateway) des serveurs et des postes utilisateurs est porté par le cœur de réseau, au nominal sur le VSS d’Alexandrin,

Les cœurs (OCCORE-VSS, DCCORE-VSS-2) ont été configurés avec une statique défaut qui pointe vers les Firewalls **Cisco ASA** (OWCASA50/ DWCASA51).

Tous les autres équipements du réseau sont des équipements effectuant uniquement de la commutation niveau 2 (pour la partie users et datacenter).

## Structure du document

Le document d’audit est structuré de la manière suivante :

* Schématique globale du réseau
* Sécurité et management des équipements
* Analyse du Layer 2
  + Vue globale du réseau
  + Analyse Cœur /distribution / access
* Analyse du Layer 3
* Performance
* Support hardware/software

Ce document décrit les configurations actuelles et les propositions d’amélioration. Pour chacune de ces améliorations, la notation suivante est utilisée :

🏱 Complexité de changement ⭘⭘⭘ | Priorité 🞊⭘⭘

Une explication du comment / pourquoi

La complexité du changement indique la difficulté technique de l’action ainsi que la consommation en temps.

⭘⭘⭘ = Facile et Rapide à 🞊🞊🞊 = Compliqué et Chronophage

La priorité du changement indique son degré d’urgence :

⭘⭘⭘ = Action non urgent à 🞊🞊🞊 = Prendre en compte rapidement le point

## Revision du document

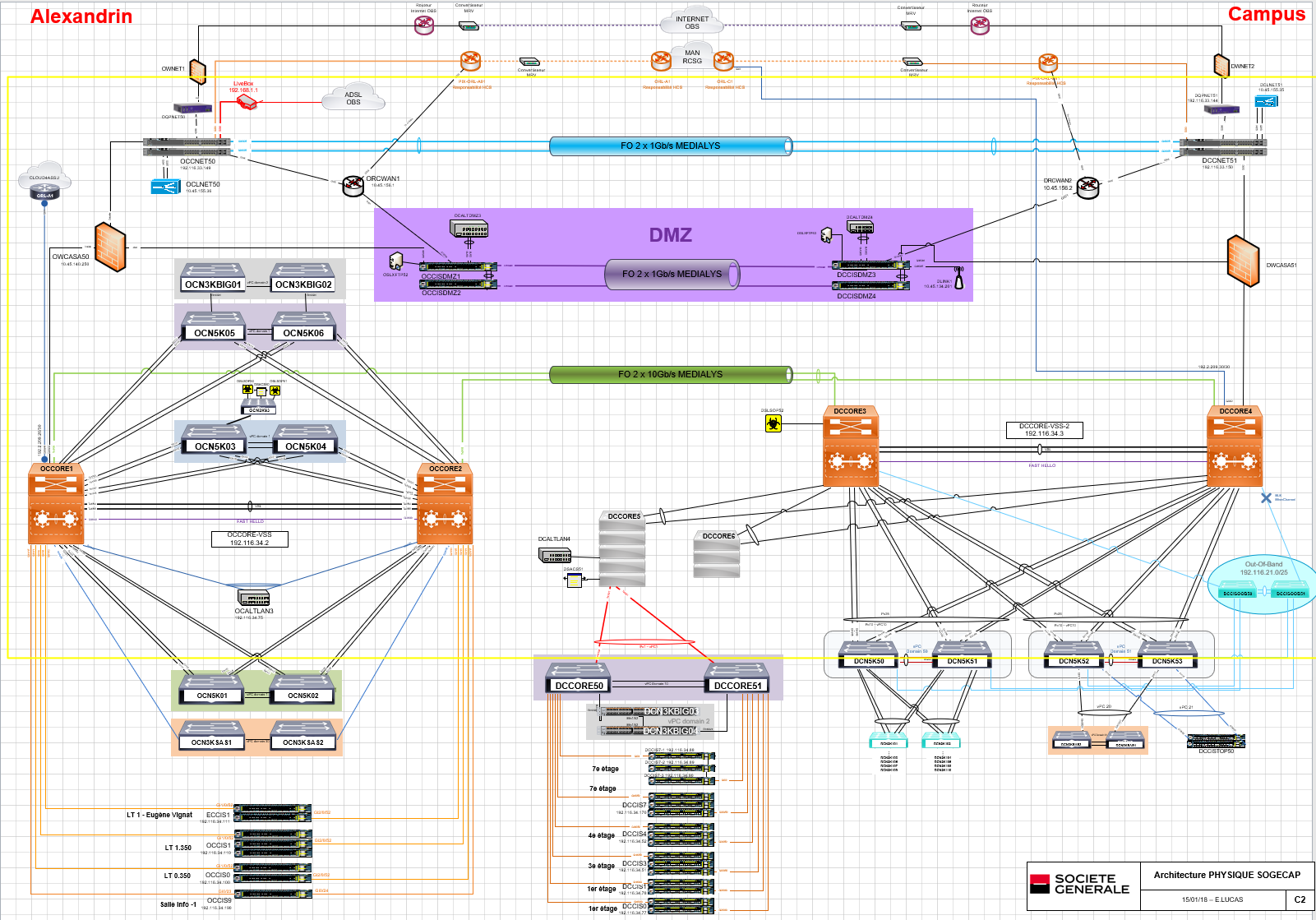
|  |  |  |
| --- | --- | --- |
| **Date** | **Author** | **Description** |
| 08/02/2018 | CHOUARHI YACINE | Draft v0.1 |
| 11/02/2018 | CHOUARHI YACINE | Draft v0.2 |
| 17/01/2016 |  |  |

# Administration

## 2. Schéma physique du réseau Sogecap Orléans

Le schéma suivant était fourni par les équipes locales en début d’audit, il représente le cœur de réseau, les zones datacenters, users ainsi DMZ.

Le périmètre de l’audit est défini en jaune sur ce schéma, a noter que cet audit est un audit réseau , un autre audit sécurité va être fourni par suite .



Il est important de donner une vision d’interconnexion avec la MAN afin de définir le sens du flux.

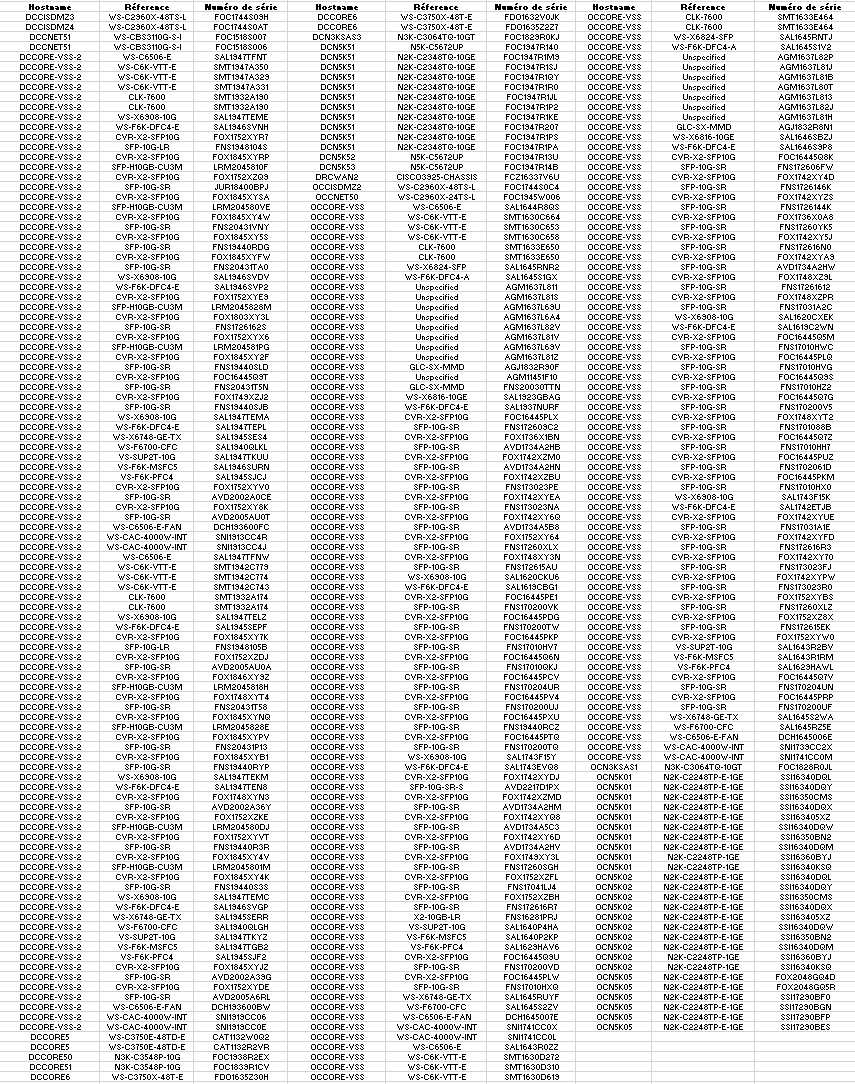


## 2.1 Inventaire opérationnel

En parallèle de Marley (base de référence Société Générale), l’ensemble des équipements actifs est référencé dans une application propriétaire Sogecap qui référence :

* Serial Number
* IOS Version
* Modèle
* Emplacement en datacenter
* Adresse IP

Voici l’inventaire sur le périmètre de l’audit :





## Monitoring des équipements

La supervision des équipements est assurée par un Nagios 4.0.8.

Il recueille les éléments suivants :

* Statut de l’équipement via simple Ping toutes les 5 minutes
* Utilisation CPU via SNMP toutes les 3 minutes
* Utilisation mémoire via SNMP toutes les 3 minutes
* Utilisation trafic via SNMP toutes les 3 minutes

La configuration des traps SNMP sur les équipements n’est pas réalisé sur tous les équipements, par exemple la liste des traps est la suivante :

### SNMP

DCCISDMZ3 | | 192.116.34.50

DCCISDMZ4 | | 192.116.34.50

DCCNET51 | | 192.116.34.50

DCCORE-VSS-2 | | 192.116.34.50

DCCORE5 | | 192.116.34.50

DCCORE50 | | 192.116.34.50

DCCORE51 | | 192.116.34.50

DCCORE6 | |

DCN3KSAS3 | | 192.116.34.50

DCN5K51 | |

DCN5K52 | |

DCN5K53 | |

DRCWAN2 | |

OCCISDMZ1 | | 192.116.34.50

OCCISDMZ2 | | 192.116.34.50

OCCNET50 | | 192.116.34.50

OCCORE-VSS | adelweb94public (RO, NONE, ANY) | 192.116.34.50

OCN3KSAS1 | | 192.116.34.50

OCN3KSAS2 | | 192.116.34.50

OCN5K01 | | 192.116.34.50

OCN5K02 | | 192.116.34.50

OCN5K05 | | 192.116.34.50

ORCWAN1 | adelweb94public (RO, NONE, ANY) | 10.45.140.4, 192.116.34.50

All SNMP communities: adelweb94public

All trap targets: 10.45.140.4, 192.116.34.50

A vérifier la configuration du snmp sur les différents équipements.

🏱 Complexité de changement 🞊⭘⭘ | Priorité 🞊⭘⭘

La configuration SNMP doit être mise en place sur tous les équipements **😊**

## Gestion des syslogs

Deux serveurs syslogs sont utilisés afin de collecter les logs des machines

* 192.116.34.50
* 192.116.34.45

La configuration actuelle des équipements Cisco est la suivante :

DCCISDMZ3 | 192.116.34.45, 192.116.34.50

DCCISDMZ4 | 192.116.34.45, 192.116.34.50

DCCNET51 | 192.116.34.45, 192.116.34.50

DCCORE-VSS-2 | 192.116.34.45, 192.116.34.50

DCCORE5 | 192.116.34.45, 192.116.34.50

DCCORE50 | 192.116.34.45, 192.116.34.50

DCCORE51 | 192.116.34.45, 192.116.34.50

DCCORE6 | 192.116.34.45, 192.116.34.50

DCN3KSAS3 | 192.116.34.45, 192.116.34.50

DCN5K51 | 192.116.34.45, 192.116.34.50

DCN5K52 | 192.116.34.45, 192.116.34.50

DCN5K53 | 192.116.34.45, 192.116.34.50

DRCWAN2 | 192.116.34.45, 192.116.34.50

OCCISDMZ1 | 192.116.34.45, 192.116.34.50

OCCISDMZ2 | 192.116.34.45, 192.116.34.50

OCCNET50 | 192.116.34.45, 192.116.34.50

OCCORE-VSS | 192.116.34.50, 192.168.34.45

OCN3KSAS1 | 192.116.34.45, 192.116.34.50

OCN3KSAS2 | 192.116.34.45, 192.116.34.50

OCN5K01 | 192.116.34.45, 192.116.34.50

OCN5K02 | 192.116.34.45, 192.116.34.50

OCN5K05 | 192.116.34.45, 192.116.34.50

ORCWAN1 | 192.116.34.45, 192.116.34.50

🏱 Complexité de changement ⭘⭘⭘ | Priorité ⭘⭘⭘

Toutes les machines envoient correctement les logs vers les deux machines de Syslog **😊**

## NTP

Un grand nombre de vulnérabilité affecte le service NTP de l’IOS et du NXOS.

Il est possible avec un paquet NTP corrompu de faire crasher les équipements, en fonction de leurs versions.

La configuration actuelle des équipements Cisco est la suivante :

DCCISDMZ3 | 10.45.1.1[4], 10.45.1.2[4]

DCCISDMZ4 | 10.45.1.1[4], 10.45.1.2[4]

DCCNET51 | 10.45.1.1[4], 10.45.1.2[4]

DCCORE-VSS-2 | 192.116.0.1[3], 192.116.0.2[4]

DCCORE5 | 10.45.1.1[4], 10.45.1.2[4]

DCCORE50 | 10.45.1.1[5], 10.45.1.2[5]

DCCORE51 | 10.45.1.1[4], 10.45.1.2[4]

DCCORE6 | 10.45.1.1[4], 10.45.1.2[4]

DCN3KSAS3 | 10.45.1.1[4], 10.45.1.2[4]

DCN5K51 | 192.116.0.1[3], 192.116.0.2[4]

DCN5K52 | 192.116.0.1[3], 192.116.0.2[4]

DCN5K53 | 192.116.0.1[3], 192.116.0.2[4]

DRCWAN2 | 10.45.1.1[4], 10.45.1.2[4]

OCCISDMZ1 | 10.45.1.1[4], 10.45.1.2[4]

OCCISDMZ2 | 10.45.1.1[4], 10.45.1.2[4]

OCCNET50 | 10.45.1.1[4], 10.45.1.2[4]

OCCORE-VSS | 192.116.0.1[3], 192.116.0.2[4]

OCN3KSAS1 | 10.45.1.1[4], 10.45.1.2[4]

OCN3KSAS2 | 10.45.1.1[4], 10.45.1.2[4]

OCN5K01 | 192.116.0.1[3], 192.116.0.2[4]

OCN5K02 | 10.45.1.1[4], 10.45.1.2[4]

OCN5K05 | 10.45.1.1[4], 10.45.1.2[4]

ORCWAN1 | 10.45.1.1[4], 10.45.1.2[4]

Quelques équipements ne sont pas synchros avec le serveur NTP, exemple :

DCCISDMZ3#show ntp status

Clock is **unsynchronized**, stratum 16, no reference clock

DCCNET51#show ntp status

Clock is **unsynchronized**, stratum 16, no reference clock

OCCISDMZ1#show ntp status

Clock is unsynchronized, stratum 16, no reference clock

De plus, si l’équipement reboot pour une certaine raison, l'horloge du logiciel serait resynchronisée avec l'horloge matérielle au démarrage et reviendrait à l'heure incorrecte. Nous pourrions régler l'horloge matérielle manuellement à l'aide du jeu de calendriers de commande, mais étant donné que l'horloge logicielle a déjà été définie, nous pouvons utiliser la commande update update-calendar pour synchroniser l'horloge matérielle sur l'horloge logicielle :

**ntp update-calendar**

🏱 Complexité de changement 🞊⭘⭘ | Priorité 🞊🞊⭘

Revoir la configuration des équipements afin de permettre la synchro NTP, de plus Il faut rajouter, une ACL protégeant les équipements contre les paquets NTP illégitimes

ntp access-group peer <ACL> **☹**

ntp update-calendar

# Sécurité des équipements

## SNMP

La configuration SNMP est homogène , néanmoins on note l’absence du snmp server sur les quelques équipements ..

Un grand nombre de Bugs (surtout sur Nexus) est lié à du SNMP polling, il est donc important de parfaitement maîtriser et limiter les serveurs qui interrogent les équipements.

### SNMP

DCCISDMZ3 | | 192.116.34.50

DCCISDMZ4 | | 192.116.34.50

DCCNET51 | | 192.116.34.50

DCCORE-VSS-2 | | 192.116.34.50

DCCORE5 | | 192.116.34.50

DCCORE50 | | 192.116.34.50

DCCORE51 | | 192.116.34.50

DCCORE6 | |

DCN3KSAS3 | | 192.116.34.50

DCN5K51 | |

DCN5K52 | |

DCN5K53 | |

DRCWAN2 | 10.45.140.4, 10.45.72.34, 192.116.34.50

OCCISDMZ1 | | 192.116.34.50

OCCISDMZ2 | | 192.116.34.50

OCCNET50 | | 192.116.34.50

OCCORE-VSS | 192.116.34.50

OCN3KSAS1 | | 192.116.34.50

OCN3KSAS2 | | 192.116.34.50

OCN5K01 | | 192.116.34.50

OCN5K02 | | 192.116.34.50

OCN5K05 | | 192.116.34.50

ORCWAN1 | 10.45.140.4, 192.116.34.50

All SNMP communities: adelweb94public

All trap targets: 10.45.140.4, 10.45.72.34, 192.116.34.50

Pour permettre à un périphérique d'envoyer des notifications SNMP (Simple Network Management Protocol) lorsque l'utilisation de la mémoire atteint un nouveau pic , utilisez la commande **'snmp-server enable traps memory**' en mode de configuration globale.

🏱 Complexité de changement ⭘⭘⭘ | Priorité 🞊🞊⭘

**snmp-server enable traps memory** permet d’envoyer des notifications si mémoire atteint un nouveau pic.

Configurer un Access List pour le SNMP.

Configurer un serveur snmp sur les équipements manquants **☹**

## Accès ACL des équipements

De manière générale, le SSH est bien la seule manière de connexion aux équipements.

L’access-list 40 est bien positionnée sur toutes les lines VTY des équipements IOS, elle n’est pas strictement identique, mais les matchs sont bien les mêmes : # Security ACL

DRCWAN2 have the following ACL 40:

===

access-list 40 permit 10.45.38.13 log

access-list 40 permit 192.116.93.232 0.0.0.7

access-list 40 permit 192.116.34.0 0.0.0.255 log

access-list 40 permit 192.116.170.0 0.0.0.255 log

access-list 40 permit 10.45.140.0 0.0.0.255 log

===

DCCORE5, DCCORE6 have the following ACL 40:

===

access-list 40 permit 10.92.0.200 log

access-list 40 permit 10.92.0.201 log

access-list 40 permit 192.116.34.0 0.0.0.255 log

access-list 40 permit 10.45.72.0 0.0.0.255 log

access-list 40 permit 10.45.140.0 0.0.0.255 log

access-list 40 permit 10.92.140.0 0.0.0.255 log

access-list 40 permit 192.116.93.0 0.0.0.255 log

access-list 40 permit 192.116.170.0 0.0.0.255 log

===

DCCNET51 have the following ACL 40:

===

access-list 40 permit 192.116.34.0 0.0.0.255 log

access-list 40 permit 192.116.170.0 0.0.0.255 log

access-list 40 permit 192.116.93.0 0.0.0.255 log

===

DCCISDMZ3, DCCISDMZ4 have the following ACL 40:

===

access-list 40 permit 192.116.170.50 log

access-list 40 permit 192.116.34.0 0.0.0.255 log

access-list 40 permit 192.116.33.128 0.0.0.31 log

access-list 40 permit 192.116.93.0 0.0.0.255 log

===

OCCISDMZ1, OCCISDMZ2, OCCNET50, OCCORE-VSS, ORCWAN1 have the following ACL 40:

===

access-list 40 permit 10.45.68.13 log

access-list 40 permit 192.116.93.232 0.0.0.7 log

access-list 40 permit 192.116.34.0 0.0.0.255 log

access-list 40 permit 192.116.170.0 0.0.0.255 log

access-list 40 permit 10.45.140.0 0.0.0.255 log

Cependant, les équipements Nexus n’ont pas de limitation sur les accès CLI :

===

# Line configuration

DCN5K51, DCN5K52, DCN5K53 have the following line configuration:

===

line console

line vty

===

DCCORE50, DCCORE51, DCN3KSAS3, OCN3KSAS1, OCN3KSAS2, OCN5K01, OCN5K02, OCN5K05 have the following line configuration:

===

line console

exec-timeout 60

line vty

exec-timeout 15

il est recommandé de passe en ssh version 2.

🏱 Complexité de changement ⭘⭘⭘ | Priorité 🞊🞊⭘

La configuration line des équipements : DCN5K51, DCN5K52, DCN5K53, DCCORE50, DCCORE51, DCN3KSAS3, OCN3KSAS1, OCN3KSAS2, OCN5K01, OCN5K02, OCN5K05 est à compléter, et l’Access List 40 à rajouter **☹.**

le ssh version 2 est recommandé ( ip ssh version 2 ).

## Serveurs HTTP / HTTPS

L’ensemble des serveurs http et HTTPS sont bien désactivé.

## Configuration Radius

Deux serveurs radius sont définis :

* 192.116.34.15
* 192.116.34.16

Les serveurs radius fournissent les services d’authentification et d’accounting.

Cependant, le service d’autorisation n’est pas fourni par les serveurs radius, ce qui a pour conséquence que les droits des users nécessitent une configuration sur les équipements (cf chapitre ci-dessous).

Il est recommandé de Migrer vers le tacacas au lieu de Radius pour avoir l’authentification AAA.

🏱 Complexité de changement 🞊🞊⭘ | Priorité 🞊🞊🞊

La configuration du service d’autorisation (aaa authorization) doit être rajoutée sur les équipements, et les serveurs radius doivent être configurés afin de fournir les droits des utilisateurs

## Utilisateurs locaux

Du fait de la configuration radius, les comptes locaux sont normalement un « backup » en cas de perte du service radius.

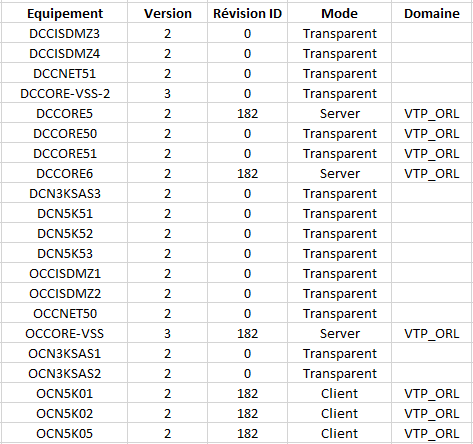
Actuellement, les droits des users sont forcés à 15 (privilège maximum) sur les équipements IOS, et sur les équipements NxOS, des comptes locaux identiques aux comptes radius sont créés afin de positionner le rôle (privilège) des utilisateurs.

La configuration est bien respectée sur la totalité du périmètre de cet audit.

# Layer 2

## VTP

Le VTP est activé à travers le réseau pour les équipements Cisco. Le statut VTP pour les équipements est le suivant :



On notera que toutes les révisions ID sont identiques pour les équipements en client / serveur ce qui est la preuve que la propagation VTP fonctionne correctement et que s’est bien synchronisé.

Cependant, il y a quelques points d’améliorations :

* L’équipement OCCORE-VSS est le seul à fonctionner en VTP V3 (rétro-compatible en V2) alors que tous les autres fonctionnent en V2.
* Certains équipements sont en mode transparent avec le domaine VTP et d’autres non.
* Il y a 3 serveurs VTP dont des équipements d’accès.
* Il est recommandé d’être en VTP version 3 vu la vulnérabilité du VTP version 2 quand on insert un nouveau client avec un Révision ID plus élevé.
* 🏱 Complexité de changement 🞊⭘⭘ | Priorité 🞊🞊🞊
* Ajouter le nom du domaine (ou le supprimer) sur tous les équipements en mode transparent.

## Mode Spanning-tree

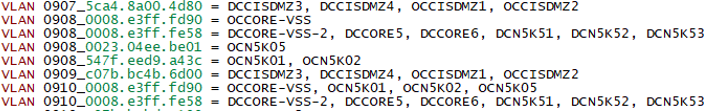
Tous les équipements fonctionnent en mode RSTP.

## Domaine Spanning-tree

L’analyse des lasts TCN prouvent que le réseau est globalement stable.

L’utilisation du VTP associé à du pruning de vlan sur les trunks (switchport trunk permit vlan) à créer des ruptures de domaine spanning-tree.

Pour illustrer :



Pour le vlans 908, nous avons donc deux root : OCN5K05 et OCCORE-VSS

Sur le OCCORE-VSS on n’autorise pas le vlan 908 sur l’interface Po54 vers le OCN5K05 .

OCCORE-VSS#

!

interface Port-channel54

description OCN5K05-OCN5K06

switchport

switchport trunk native vlan 998

switchport trunk allowed vlan 1-17,19,20,30,54,60-64,80,81,89,97,99,130,140

switchport trunk allowed vlan add 175,180-183,190,195,200-300,335-337,343-345

switchport trunk allowed vlan add 347,348,351-354,357,360,361,367,370,375,376

switchport trunk allowed vlan add 383,900,901,910-913,920,921,930,995-999

switchport mode trunk

ip dhcp snooping trust

end

Le fichier suivant identifie pour chaque vlan les root associés :

*Ex :*

VLAN 0908\_0008.e3ff.fd90 = OCCORE-VSS

VLAN 0908\_0023.04ee.be01 = OCN5K05

VLAN 0908\_547f.eed9.a43c = OCN5K01, OCN5K02

*Cet exemple montre trois instances spanning-tree pour le vlan 908 sur différents équipements , la première est présente sur les switchs* OCN5K05 qui a pour root le 0023.04ee.be01 *,* OCN5K02 qui a pour root 547f.eed9.a43c et  *et a troisième sur les switchs* OCCORE-VSS *et a pour root le* 0008.e3ff.fd90*.*

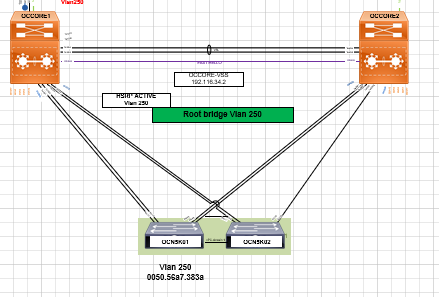
**

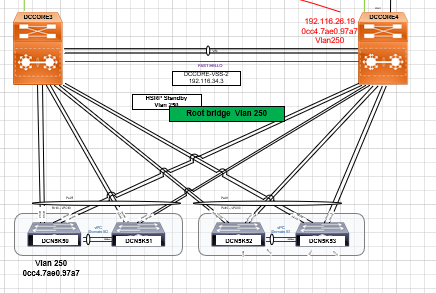
🏱 Complexité de changement 🞊🞊🞊 | Priorité 🞊⭘⭘

* Il n’est pas recommandé d’avoir des domaines spanning-tree discontinus, ce qui peut avoir des effets de convergence importants en cas d’interconnexion de ces deux domaines ou meme la création d’une boucle spanning tree
* Deux solutions sont possibles mais complexes à mettre en œuvre. 1. Supprimer le VTP et ne créer que les vlans utilisés sur les différents switchs (best practice) et ainsi n’autoriser dans les trunks que les vlans nécessaires. 2. Autoriser tous les vlans dans les trunks entre les différents switchs du domaine VTP en client/serveur et activer le vtp pruning qui va automatiquement limiter la propagation des vlans dans les trunks (solution plus rapide et moins contraignante).

## Topologie Spanning-tree

Dans la topologie fournie en début d’audit, le root spanning tree identifié est occore-vss/dccore-vss-2

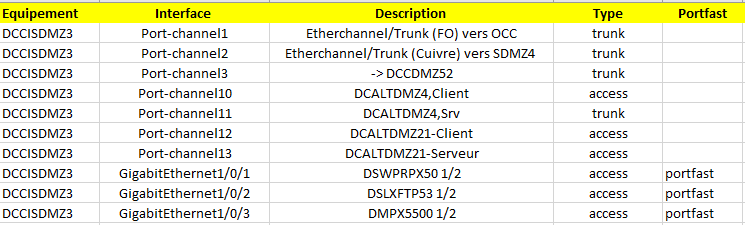




## Customisation spanning-tree

Les modes *default edge port* sur les nexus */ portfast default* sur les catalyst ne sont pas utilisés.

Le mode BPDU guard default est activé sur quelques chassis Nexus :



Exemple : DCCISDMZ3 , le port PO12 est en mode access mais n’est pas configuré en portfast .

Attention cependant aux points suivants qui concernent les ports d’accès :

* De nombreux ports ne sont pas configurés en portfast.
* La fonctionnalité bpdufilter est utilisée, celle-ci désactive totalement l’envoi/réception de bpdu sur les interfaces, ce qui peux autoriser les boucles de niveau 2 sans possibilité de les couper.

Le tableau dans le fichier joint détaille toutes les interfaces du réseau et la configuration actuelle :



🏱 Complexité de changement 🞊⭘⭘ | Priorité 🞊🞊🞊

* Configurer le portfast sur les interfaces en access ( il y a une instabilité spanning-tree)
* La fonctionnalité bpdufilter doit être retirée des interfaces d’accès . Celle-ci désactive les mécanismes de protection des boucles réseaux. Il faut préférer bpduguard, qui va désactiver le port si un bpdu est reçu.

## CDP

Le CDP est de manière générale désactivé sur le réseau, cependant certains équipements ont le CDP d’activé et d’autres n’ont que le CDP désactivé sur certaines interfaces.

Le CDP est extrêmement pratique lors de troubleshooting et la recommandation actuelle de Cisco est l’activation du CDP dans un réseau dit « trust ».

🏱 Complexité de changement ⭘⭘⭘ | Priorité ⭘⭘⭘

* Réactiver le CDP sur l’ensemble du réseau Sogecap.

## UDLD

L’ensemble des uplinks réseau a bien l’udld configuré, ce qui permet de désactiver l’interface si un fonctionnement unidirectionnel est détecté.

## Storm-control

Le storm control, permet de limiter les tempêtes sur le réseau, il est important d’avoir une politique de gestion.

Sur certaines configurations (ocn5k01/02), celle-ci est configurée sur quelques interfaces.

Il est a noté que dans le cadre de cette audit, on ne peut pas auditer les équipements en accès ( pas de droit d’accès)

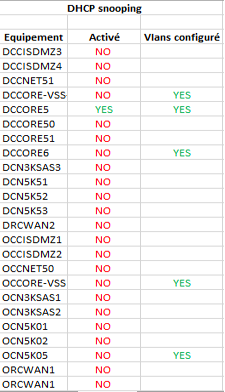
La recommandation actuelle de Cisco est la configuration au port d’accès.

🏱 Complexité de changement 🞊🞊🞊 | Priorité 🞊🞊⭘

* Il faut définir une politique uniforme de storm control et l’appliquer sur l’ensemble des équipements.

## DHCP snooping

Le DHCP snooping est configuré sur une partie des équipements, cependant malgré la présence de configurations, il n’est pas forcément activé (commande « ip dhcp snooping » manquante en global) .



Le fichier ci-joint liste les vlans ou le dhcp snooping est configuré :



🏱 Complexité de changement 🞊🞊⭘ | Priorité 🞊⭘⭘

* Le dhcp snooping est un best-practice, il doit être configuré sur tous les vlans. Les ports légitimes (accès vers les serveurs dhcp et uplink) doivent être positionnés en trust. Le fichier en joint liste aussi les interfaces en ip dhcp snooping trust. Une passe sur la légitimité de ces interfaces est à réaliser.

## ARP inspection

L’arp inspection n’est pas configuré sur le réseau Sogecap.

## IGMP snooping

L’igmp snooping est bien activé sur l’ensemble des équipements réseau Sogecap.

L’IGMP querier pour l’ensemble du lan est occore-vss (ip igmp snooping querier)

* Complexité de changement 🞊⭘⭘ | Priorité 🞊🞊🞊
* Il n’y a pas de redondance configurée sur la partie querier igmp. Cette configuration doit-être réalisée sur un des deux équipements DCCORE-VSS-2 afin d’assurer la continuité du service en cas de panne de l’équipement OCCORE-VSS.

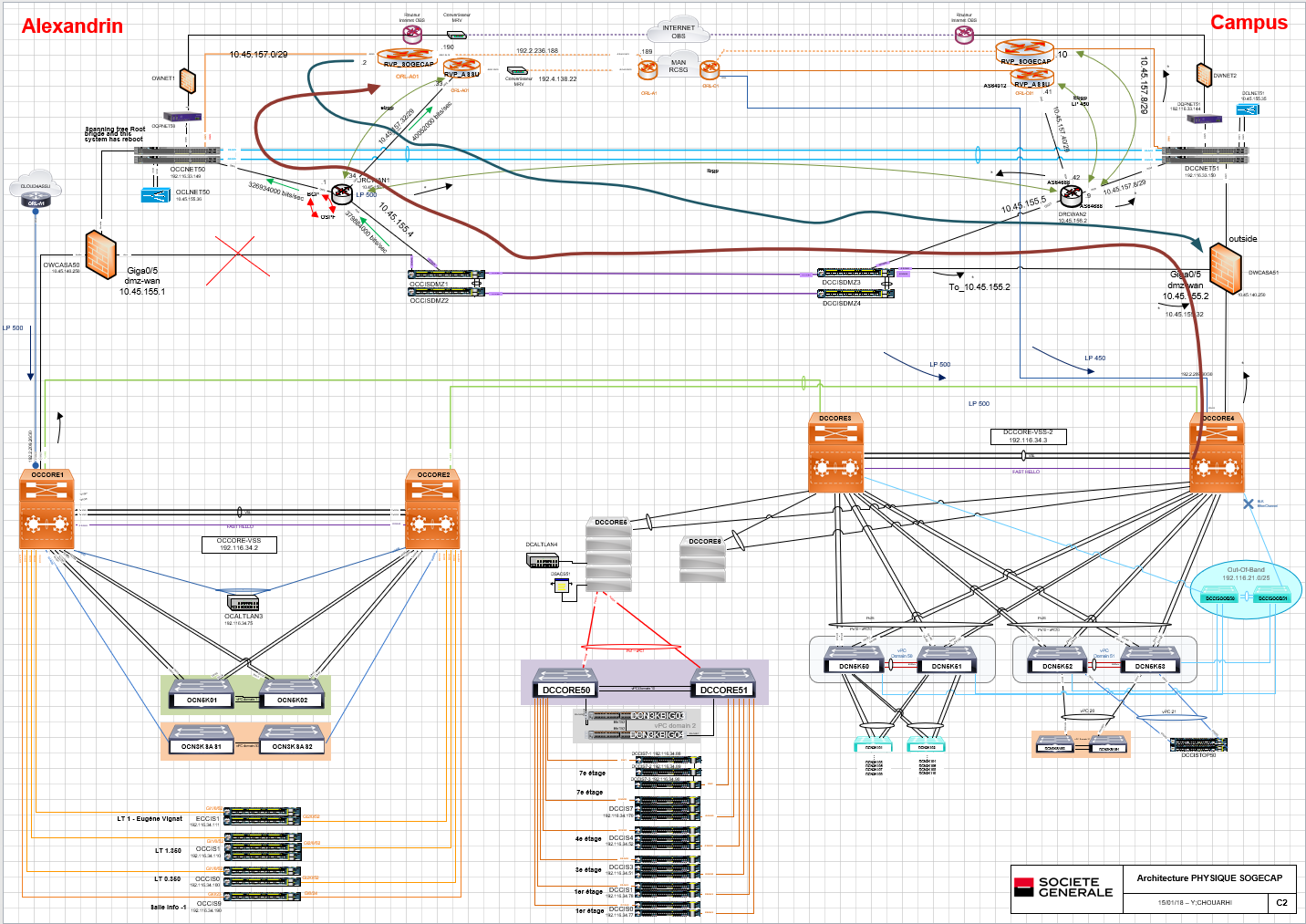
## MTU

La configuration MTU est uniforme sur le réseau et positionnée à 1500.

## Etherchannel

Les liens sont en LACP ce qui permet de détecter les erreurs

# Layer 3



## Routage Statique

L’ensemble du routage est porté par les deux équipements :

* OCCORE-VSS
* DCCORE-VSS-2

On retrouve les routes statiques suivants :

occore-vss:ip route 0.0.0.0 0.0.0.0 10.45.140.250

occore-vss:ip route 10.45.32.0 255.255.255.0 10.45.10.230 name ALTEON\_LAN

occore-vss:ip route 10.45.156.101 255.255.255.255 192.116.34.3

occore-vss:ip route 192.116.12.209 255.255.255.255 Vlan221

occore-vss:ip route 192.116.19.6 255.255.255.255 Vlan230

occore-vss:ip route 192.116.19.20 255.255.255.255 Vlan230

occore-vss:ip route 192.116.19.21 255.255.255.255 Vlan230

occore-vss:ip route 192.116.19.35 255.255.255.255 Vlan230

occore-vss:ip route 192.116.19.135 255.255.255.255 Vlan230

occore-vss:ip route 192.116.21.0 255.255.255.128 192.116.34.3 name OOB\_CAMPUS

occore-vss:ip route 192.116.31.0 255.255.255.0 192.116.9.9 name ALTEON\_LAN\_PRE\_PROD

occore-vss:ip route 192.116.31.100 255.255.255.255 192.116.9.11

occore-vss:ip route 192.116.32.0 255.255.255.0 10.45.10.230 name ALTEON\_LAN\_SGNA

occore-vss:ip route 192.116.33.160 255.255.255.240 10.45.140.250

occore-vss:ip route 192.116.34.200 255.255.255.255 Vlan210

occore-vss:ip route 192.117.0.0 255.255.240.0 192.116.34.3

dccore-vss-2:ip route 0.0.0.0 0.0.0.0 10.45.140.250

dccore-vss-2:ip route 10.45.32.0 255.255.255.0 10.45.10.230 name ALTEON\_LAN

dccore-vss-2:ip route 10.45.156.100 255.255.255.255 192.116.34.2

dccore-vss-2:ip route 192.116.12.209 255.255.255.255 Vlan221

dccore-vss-2:ip route 192.116.19.135 255.255.255.255 Vlan230

dccore-vss-2:ip route 192.116.31.0 255.255.255.0 192.116.9.9 name ALTEON\_LAN\_PRE\_PROD

dccore-vss-2:ip route 192.116.32.0 255.255.255.0 10.45.10.230 name ALTEON\_LAN\_SGNA

dccore-vss-2:ip route 192.116.34.200 255.255.255.255 Vlan210

* Complexité de changement ⭘⭘⭘ | Priorité 🞊🞊🞊
* Homogénéiser les routes sur les 2 vss, actuellement les routes suivantes sont absentes des deux équipements portant le routage backup :

ip route 192.116.19.6 255.255.255.255 Vlan230

ip route 192.116.19.20 255.255.255.255 Vlan230

ip route 192.116.19.21 255.255.255.255 Vlan230

ip route 192.116.19.35 255.255.255.255 Vlan230

ip route 192.116.21.0 255.255.255.128 192.116.34.3 name OOB\_CAMPUS

ip route 192.116.31.100 255.255.255.255 192.116.9.11

ip route 192.116.33.160 255.255.255.240 10.45.140.250

ip route 192.117.0.0 255.255.240.0 192.116.34.3

## Routage Dynamique

## 5.2.1 OSPF

Le routage OSPF est activé entre les routeurs ORCWAN1/ DRCWAN2 et les firewalls Cisco ASA OWCASA50/DWCASA51 dans l’area 0.

Le routeurs ORCWAN1/ DRCWAN2 représentent des ASBR connectés en BGP au RCSG MAN.

A noter, l’existence du HSRP et l’OSPF sur le même segment, la présence seul de l’OSPF peut fournir la résilience, par conséquent le fonctionnement de l’HSRP attendu n’a pas d’utilité dans ce cas de figure.

De plus, on note l’existence du PBR et des routes-map avec un Access-List qui ne match aucune entrée.

ORCWAN1#

interface GigabitEthernet0/1

description OCCISDMZ1,g1/0/34

ip address 10.45.155.4 255.255.255.240

standby 1 ip 10.45.155.3

standby 1 priority 200

standby 1 preempt

standby 1 track 1 decrement 50

ip policy route-map PBR

ip ospf dead-interval 10

ip ospf hello-interval 2

route-map PBR permit 10

match ip address PBR\_To\_RIX

set ip next-hop verify-availability 10.45.157.33 2 track 2

set ip next-hop verify-availability 10.45.155.22 3 track 3

route-map PBR permit 20

match ip address PBR\_To\_PAX

set ip next-hop verify-availability 10.45.157.2 10 track 4

set ip next-hop verify-availability 10.45.155.5 30 track 3

les access-list:

ip access-list extended PBR\_To\_PAX

deny ip host 192.116.148.64 any

deny ip 192.116.27.0 0.0.0.255 any

deny ip 192.116.21.0 0.0.0.255 any

deny ip 192.116.128.0 0.0.63.255 any

deny ip 192.117.0.0 0.0.63.255 any

deny ip 192.117.64.0 0.0.7.255 any

ip access-list extended PBR\_To\_RIX

permit ip host 192.116.148.64 any

permit ip 192.116.27.0 0.0.0.255 any

permit ip 192.116.21.0 0.0.0.255 any

permit ip 192.116.128.0 0.0.63.255 any

permit ip host 192.117.40.8 any log

permit ip host 192.117.0.37 any log

permit ip 192.117.0.0 0.0.63.255 any

permit ip 192.117.64.0 0.0.7.255 any

l’ACL **PBR\_To\_PAX** contient que des lignes en Deny (avec un implicite deny à la fin ) , cet Access List n’a forcément pas d’utilité .

On trouve la même configuration sur le site DR :

DRCWAN2#

interface GigabitEthernet0/1

description DQPWAN OUTSIDE

ip address 10.45.155.5 255.255.255.240

standby 1 ip 10.45.155.3

standby 1 priority 150

standby 1 preempt

standby 1 track 1 decrement 50

ip policy route-map PBR

ip ospf dead-interval 10

ip ospf hello-interval 2

route-map PBR permit 10

match ip address PBR\_To\_RIX

set ip next-hop verify-availability 10.45.157.41 20 track 2

set ip next-hop verify-availability 10.45.155.4 30 track 3

route-map PBR permit 20

match ip address prefix-list PBR\_To\_PAX

set ip next-hop verify-availability 10.45.157.10 10 track 4

set ip next-hop verify-availability 10.45.155.4 30 track 3

l’ACL :

ip access-list extended PBR\_To\_PAX

**deny ip 192.116.27.0 0.0.0.255 any**

**deny ip 192.116.21.0 0.0.0.255 any**

**deny ip 192.116.128.0 0.0.63.255 any**

**deny ip 192.117.0.0 0.0.255.255 any**

ip access-list extended PBR\_To\_RIX

deny ip any any

permit ip 192.116.27.0 0.0.0.255 any

permit ip 192.116.21.0 0.0.0.255 any

permit ip 192.116.128.0 0.0.63.255 any

permit ip 192.117.0.0 0.0.255.255 any

l’ACL n’est pas homogène sur les deux équipements ORCWAN2/DRCWAN2

DRCWAN2#show ip access-lists PBR\_To\_RIX

Extended IP access list PBR\_To\_RIX

5 deny ip any any (17434 matches)

10 permit ip 192.116.27.0 0.0.0.255 any

20 permit ip 192.116.21.0 0.0.0.255 any

30 permit ip 192.116.128.0 0.0.63.255 any (128476629 matches)

40 permit ip 192.117.0.0 0.0.255.255 any (209857044 matches)

À la suite de l’incident du Mercredi 16/01/2019 et 30/01/2019, nous avons trouvé un **top Talker** qui a l’adresse 192.116.26.123. Après isolation, le service est revenu à la normal, nous avons déduit que l’incident du 12 décembre et ce dernier sont lies.

La redistribution des routes statiques dans l’OSPF n’est pas homogène dans les ACL.

OCCORE-VSS#

router ospf 1

redistribute static subnets route-map RM\_ORL\_To\_COL

DCCORE-VSS-2#

router ospf 1

redistribute static subnets route-map RM\_ORL\_To\_COL

les ACL ne sont pas homogène sur les deux CORE:

OCCORE-VSS#

ip access-list extended TSM6\_7\_et\_NIM

permit ip host 192.116.19.230 any

permit ip host 192.116.19.20 any

permit ip host 192.116.19.6 any

permit ip host 192.116.19.35 any

permit ip host 192.116.34.200 any

permit ip host 192.116.19.135 any

permit ip host 192.116.34.50 any

permit ip host 192.116.12.209 any

permit ip host 192.116.19.21 any

DCCORE-VSS-2#

ip access-list extended TSM6\_7\_et\_NIM

permit ip host 192.116.19.20 any

permit ip host 192.116.19.35 any

permit ip host 192.116.34.200 any

permit ip host 192.116.19.135 any

permit ip host 192.116.12.209 any

match ip address TSM6\_7\_et\_NIM

* Complexité de changement ⭘⭘⭘ | Priorité 🞊🞊⭘
* Nécessite de Faire un clean de la configuration HSRP, peut-être il s’agit d’un oubli suite à une migration vers l’OSPF .
* Homogénéiser la configuration des ACL TSM6\_7\_et\_NIM sur les deux équipements
* Vérifier la configuration du PBR (ACL… ) configure sur les deux ORCWAN1 et DRCWAN2
* Homogénéiser les routes sur les 2 vss, actuellement les routes suivantes sont absentes des deux équipements portant le routage backup :

ip route 192.116.19.6 255.255.255.255 Vlan230

ip route 192.116.19.20 255.255.255.255 Vlan230

ip route 192.116.19.21 255.255.255.255 Vlan230

ip route 192.116.19.35 255.255.255.255 Vlan230

ip route 192.116.21.0 255.255.255.128 192.116.34.3 name OOB\_CAMPUS

ip route 192.116.31.100 255.255.255.255 192.116.9.11

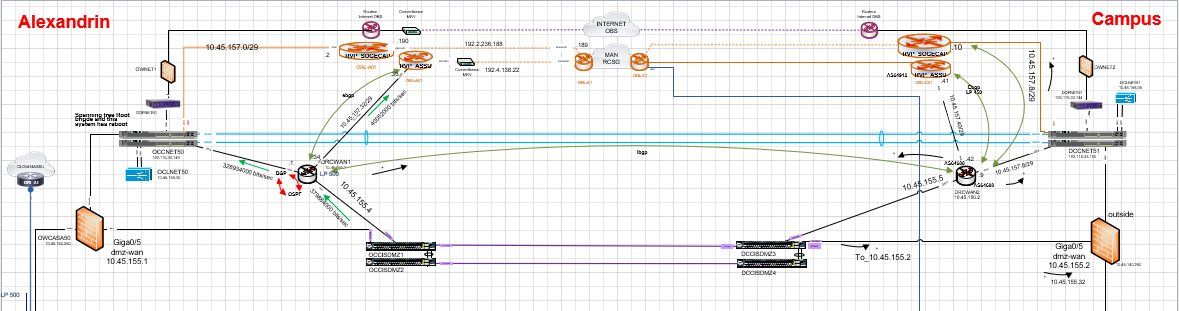
ip route 192.116.33.160 255.255.255.240 10.45.140.250

ip route 192.117.0.0 255.255.240.0 192.116.34.3

## 5.3 BGP

ORCWAN1/DRCWAN2 ont trois sessions BGP, deux sessions ebgp (AS 64912) avec le MAN SG et une session iBGP (AS 64688 ) en interne .

ORCWAN1 annonce les routes avec un local Préférence de 500 contrairement au DRCWAN2 , le local Préférence est de 450.



ORCWAN1 annonce la route par default vers le SOGECAP ( RVP\_SOGECAP ) , le LAN ASSU Orléans représente un réseau de transit pour SOGECAP .

La configuration du BGP est symétrique dans les deux sites, les routes annoncés sont homogènes de part et d’autre

ORCWAN1#show ip cef traffic prefix-length

Forwarding tree:

Per-prefix length statistics:

Mask Lookups Inserts Deletes Current

Length (disabled) (disabled) (disabled) (enabled)

0 0 0 0 1

1 0 0 0 0

2 0 0 0 0

3 0 0 0 0

4 0 0 0 2

5 0 0 0 0

6 0 0 0 0

7 0 0 0 0

8 0 0 0 2

9 0 0 0 0

10 0 0 0 0

11 0 0 0 0

12 0 0 0 0

13 0 0 0 0

14 0 0 0 1

15 0 0 0 0

16 0 0 0 45

17 0 0 0 0

18 0 0 0 6

19 0 0 0 0

20 0 0 0 1

21 0 0 0 27

22 0 0 0 11

23 0 0 0 28

24 0 0 0 523

25 0 0 0 12

26 0 0 0 9

27 0 0 0 10

28 0 0 0 19

29 0 0 0 8

30 0 0 0 47

31 0 0 0 0

32 0 0 0 167

DRCWAN2#show ip cef traffic prefix-length

Forwarding tree:

Per-prefix length statistics:

Mask Lookups Inserts Deletes Current

Length (disabled) (disabled) (disabled) (enabled)

0 0 0 0 1

1 0 0 0 0

2 0 0 0 0

3 0 0 0 0

4 0 0 0 2

5 0 0 0 0

6 0 0 0 0

7 0 0 0 0

8 0 0 0 2

9 0 0 0 0

10 0 0 0 0

11 0 0 0 0

12 0 0 0 0

13 0 0 0 0

14 0 0 0 1

15 0 0 0 0

16 0 0 0 45

17 0 0 0 0

18 0 0 0 6

19 0 0 0 0

20 0 0 0 1

21 0 0 0 27

22 0 0 0 11

23 0 0 0 28

24 0 0 0 522

25 0 0 0 12

26 0 0 0 9

27 0 0 0 10

28 0 0 0 19

29 0 0 0 8

30 0 0 0 47

31 0 0 0 0

32 0 0 0 167

De plus, il faut penser à retirer la command soft-reconfiguration inbound, cette commande va chercher de la mémoire pour faire une copie des routes reçues.

ORCWAN1

router bgp 64688

!

address-family ipv4

neighbor 10.45.156.2 soft-reconfiguration inbound

neighbor 10.45.157.2 soft-reconfiguration inbound

neighbor 10.45.157.33 soft-reconfiguration inbound

DRCWAN2#

router bgp 64688

!

address-family ipv4

neighbor 10.45.156.1 soft-reconfiguration inbound

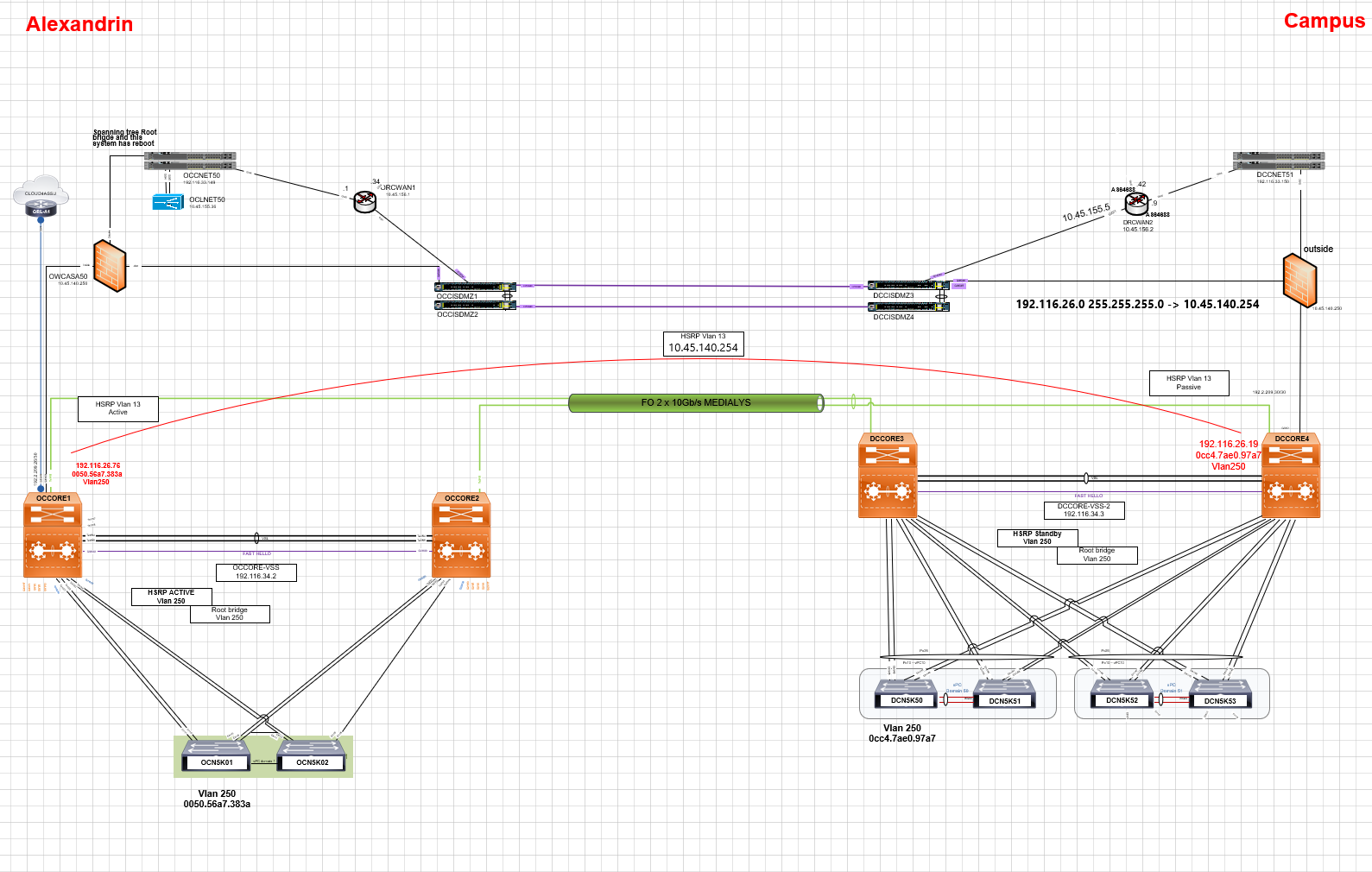
neighbor 10.45.157.10 soft-reconfiguration inbound

neighbor 10.45.157.41 soft-reconfiguration inbound

il faut utiliser la feature BGP Soft Reset Enhancement à la place du soft-reconfiguration inbound .

<https://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/s_sftrst.html#wp1034996>

## HSRP



Le HSRP est configuré donne le but d’offrir la résilience entre les deux vss (OCCORE-VSS/ DCCORE-VSS-2).

Au moment de la rédaction de ce guide, le vss OCCORE-VSS est active pour l’ensemble des Vlans .

OWCASA50# show route | i 10.45.140.254

S 10.45.0.0 255.255.0.0 [1/0] via 10.45.140.254, inside

S 10.46.0.0 255.255.255.0 [1/0] via 10.45.140.254, inside

OCCORE-VSS#show running-config interface vlan 13

!

interface Vlan13

description Management

ip address 10.45.140.253 255.255.255.0

ip helper-address 192.116.34.11

ip helper-address 192.116.34.13

no ip redirects

no ip unreachables

standby 13 ip 10.45.140.254

standby 13 priority 120

standby 13 preempt

arp timeout 300

OCCORE-VSS#show standby brief

|

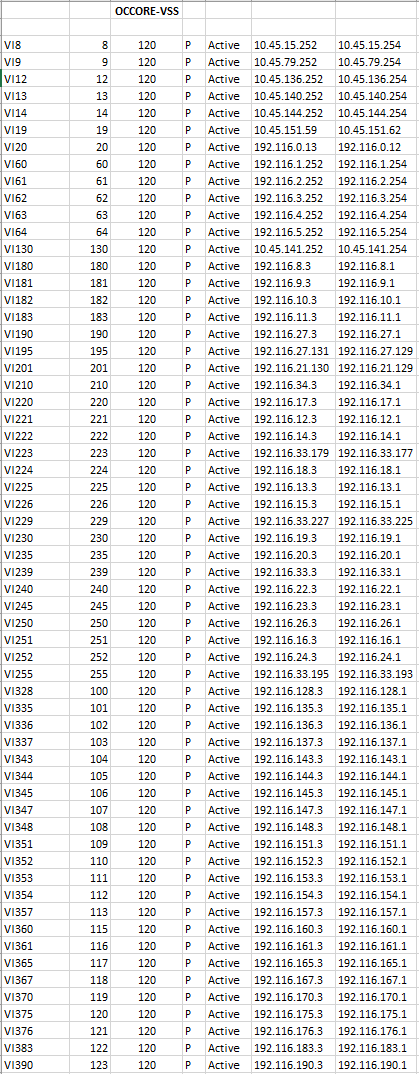
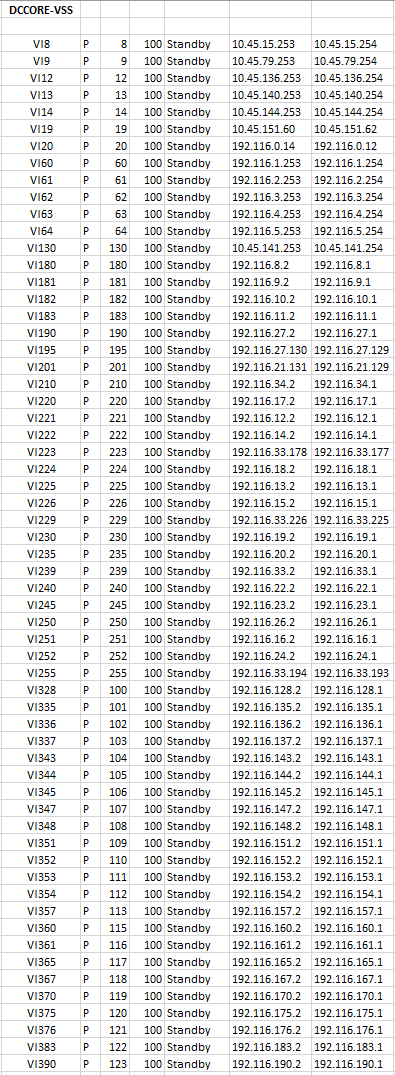
Interface Grp Pri P State Active Standby Virtual IP

Vl8 8 120 P Active local 10.45.15.252 10.45.15.254

Vl9 9 120 P Active local 10.45.79.252 10.45.79.254

Vl12 12 120 P Active local 10.45.136.252 10.45.136.254

La liste des HRSP est la suivante :

La route statique sur les Firewalls ASA pointe vers l’adresse HSRP du Vlan 13, étant donné que l’HSRP est en active sur le OCCORE-VSS , le sens du flux pour une source se trouvant dans le Vlan 250 (DCN5K51 )est :

OWCASA51 -> DCCORE-VSS-2 -> OCCORE-VSS -> DCCORE-VSS-2-> DCN5K50

Le chemin n’est donc pas optimal.

On note bien la présence du tracking sur l’adresse HSRP vlan 13 DCCORE-VSS-2, on ne trouve pas ce type de tracking sur le OCCORE-VSS

DCCORE-VSS-2#show running-config interface vlan 13

!

interface Vlan13

description Management

ip address 10.45.140.252 255.255.255.0

no ip redirects

no ip unreachables

standby 13 ip 10.45.140.254

standby 13 preempt delay minimum 30

standby 13 **track 10 decrement 30**

arp timeout 300

* Complexité de changement 🞊⭘⭘ | Priorité 🞊⭘⭘
* Afin d’avoir un chemin optimal, il faut bien être synchro en terme d’HSRP (active sur les VSS, en face de lui l’active ASA).
* Etudier la possibilité de rajouter du HSRP Track avec la bonne interface sur le OCCORE-VSS.

# Performance

## 6.1 Utilisation mémoire et CPU

Aucune alerte particulière n’a été identifiée sur les différents équipements.

## 6.2 Utilisation TCAM

L’utilisation de la mémoire TCAM est quasiment négligeable sur le châssis VSS.

Cependant la TCAM des switchs DCCORE5 et DCCORE6 est à un taux d’utilisation non négligeable :

OCCORE-VSS#show platform hardware capacity forwarding

L2 Forwarding Resources

MAC Table usage: Sw/Mod Collisions Total Used %Used

1/1 0 131072 3052 2%

1/2 0 131072 3057 2%

1/3 0 131072 3053 2%

1/4 0 131072 3053 2%

1/5 0 131072 3058 2%

2/1 0 131072 3044 2%

2/2 0 131072 3051 2%

2/3 0 131072 3044 2%

2/4 0 131072 3050 2%

2/5 0 131072 3052 2%

L3 Forwarding Resources

FIB TCAM usage: Total Used %Used

72 bits (IPv4, MPLS, EoM) 262144 3571 1%

144 bits (IP mcast, IPv6) 131072 4 1%

288 bits (IPv6 mcast) 65536 1 1%

detail: Protocol Used %Used

IPv4 3570 1%

MPLS 0 0%

EoM 1 1%

IPv6 1 1%

IPv4 mcast 3 1%

IPv6 mcast 1 1%

Adjacency usage: Total Used %Used

1048576 35228 3%

Forwarding engine load:

Sw/Mod pps peak-pps peak-time

1/1 109 86527 16:40:27 GMT+1 Wed Nov 22 2017

1/2 1280 393332 18:57:07 FR-ETE Sat May 26 2018

1/3 9083 1789328 12:07:46 GMT+1 Fri Feb 16 2018

1/4 123635 1830500 09:00:02 GMT+1 Sat Nov 11 2017

1/5 20365 980136 13:48:46 GMT+1 Wed Feb 7 2018

2/1 0 83 19:50:14 FR-ETE Mon Sep 11 2017

2/2 1332 462129 18:38:24 GMT+1 Sat Jan 5 2019

2/3 30181 1819647 02:50:57 GMT+1 Thu Feb 8 2018

2/4 72491 1479065 09:46:28 FR-ETE Sun Oct 8 2017

2/5 6783 932839 00:02:28 GMT+1 Mon Jan 8 2018

DCCORE-VSS-2#show platform hardware capacity forwarding

L2 Forwarding Resources

MAC Table usage: Sw/Mod Collisions Total Used %Used

1/1 0 131072 3052 2%

1/2 0 131072 3047 2%

1/3 0 131072 3047 2%

1/5 0 131072 3051 2%

2/1 0 131072 3049 2%

2/2 0 131072 3051 2%

2/3 0 131072 3051 2%

2/5 0 131072 3050 2%

L3 Forwarding Resources

FIB TCAM usage: Total Used %Used

72 bits (IPv4, MPLS, EoM) 262144 1425 1%

144 bits (IP mcast, IPv6) 131072 4 1%

288 bits (IPv6 mcast) 65536 1 1%

detail: Protocol Used %Used

IPv4 1424 1%

MPLS 0 0%

EoM 1 1%

IPv6 1 1%

IPv4 mcast 3 1%

IPv6 mcast 1 1%

Adjacency usage: Total Used %Used

1048576 33140 3%

Forwarding engine load:

Sw/Mod pps peak-pps peak-time

1/1 139486 1834130 10:01:20 FR-ETE Fri Aug 10 2018

1/2 1271 1648104 15:59:18 FR-ETE Mon May 14 2018

1/3 0 250 16:03:08 UTC Fri Feb 23 2018

1/5 10425 157860 10:12:59 UTC Mon Nov 26 2018

2/1 51953 1779195 14:11:41 FR-ETE Thu Aug 30 2018

2/2 3469 233750 16:46:47 FR-ETE Thu Apr 26 2018

2/3 1 250 20:00:23 FR-ETE Tue Apr 4 2017

2/5 36922 134250 13:40:57 UTC Wed Dec 26 2018

## 6.3 Erreurs sur les interfaces

Deux traces sur l’ensemble du réseau ont été prises à 24H d’intervalle afin de remonter les compteurs des interfaces.

Une différence a pu être réalisée afin de remonter les interfaces voyant leurs compteurs d’erreurs s’incrémenter, ci-dessous le fichier brut :



Ce type d’erreur observe sur les outputs sont dues :

* Output drops : erreurs quasi normales lors d’une différence de vitesse lors de la communication de deux hôtes à différentes vitesses (ex, un serveur 1Gbit/s envoyant des données sur un serveur à 100Mbit/s).
* Complexité de changement 🞊⭘⭘ | Priorité 🞊🞊⭘
* Aucune action

# Best Practice

## VSS

Le document Cisco VSS best practice recommande l’utilisation de la dual active recovery mode

<https://www.cisco.com/c/dam/global/da_dk/assets/docs/presentations/VSS_0109.pdf>.

https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Campus/VSS30dg/campusVSS\_DG/VSS-dg\_ch4.html

La perte du lien VSL donnerai naissance à ce qu’on appelle un **dual active condition**, ce phénomène va créer deux routeurs indépendants avec le même control plane ( IP adresse , router ID … ) .

Afin de lutter contre ce phénomène Cisco propose diffèrent mécanismes :

Enhanced PAgP

BFD

Fast VSLP Hello (supported in 12.2(33)SXHI)

OCCORE-VSS#show switch virtual dual-active summary

Pagp dual-active detection enabled: No

Fast-hello dual-active detection enabled: Yes

FEX dual-active detection enabled: Yes

No interfaces excluded from shutdown in recovery mode

**In dual-active recovery mode: No**

* Complexité de changement 🞊🞊⭘ | Priorité 🞊🞊⭘
* Etudier la faisabilité des mécanismes qui protège les équipements du **dual active state**

## HSRP

## 7.2.1 HSRP Authentification

Souhaitable dans la configuration du HSRP, elle peut être configurer en utilisant un clear text ou une authentification de type md5 .

## 7.2.1 Standby Delay Minimum Reload

Si le routeur actif échoue ou si vous le supprimez du réseau, le routeur de secours devient automatiquement le nouveau routeur actif. Si l'ancien routeur actif revient en ligne, vous pouvez contrôler s'il prend ou non le routeur actif à l'aide de la commande standby preempt. Toutefois, dans certains cas, même si vous n'utilisez pas la commande standby preempt, l'ancien routeur actif reprend le rôle actif. Après qu’il revient en ligne. Utilisez la commande reload minimum reload delay pour définir un délai d’initialisation du groupe HSRP. Cette commande laisse le temps aux paquets de s'écouler avant que le routeur ne reprenne le rôle actif.

**Standby delay minimum [min-delay] reload [reload-delay]**

En général Cisco recommande un min-delay=30 et reload-delay=60

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp\_fhrp/configuration/xe-3s/fhp-xe-3s-book/fhp-hsrp.html

## Mac adresse Move

Dans d’un réseau LAN  , La notification de déplacement d'adresse MAC détecte les défaillances possibles du réseau en enregistrant les déplacements MAC à l'aide des syslog et / ou SNMP. Les déplacements fréquents d'hôtes ne devraient normalement pas se produire dans un réseau stable. Un nombre élevé de déplacements MAC peut indiquer une éventuelle boucle ou un hôte mal configuré.

**mac-address-table notification mac-move**

## 