

Monitoring Réseau Bureautique & Gain de temps



Linda TCHIDAT

PLAN

1 SITUATION DE DÉPART (Réf ITIL)

2 CHALLENGE

3 ASTUCE

4 EXEMPLE

5 BÉNÉFICES

FRENCH

ZABBIX 

MEETUP ONLINE '20

Situation de départ (réf ITIL)

INCIDENT



Situation de départ (réf ITIL)

INCIDENT

Description

Événement n'appartenant pas au fonctionnement standard d'un service et susceptible de perturber les opérations normales de l'utilisateur final

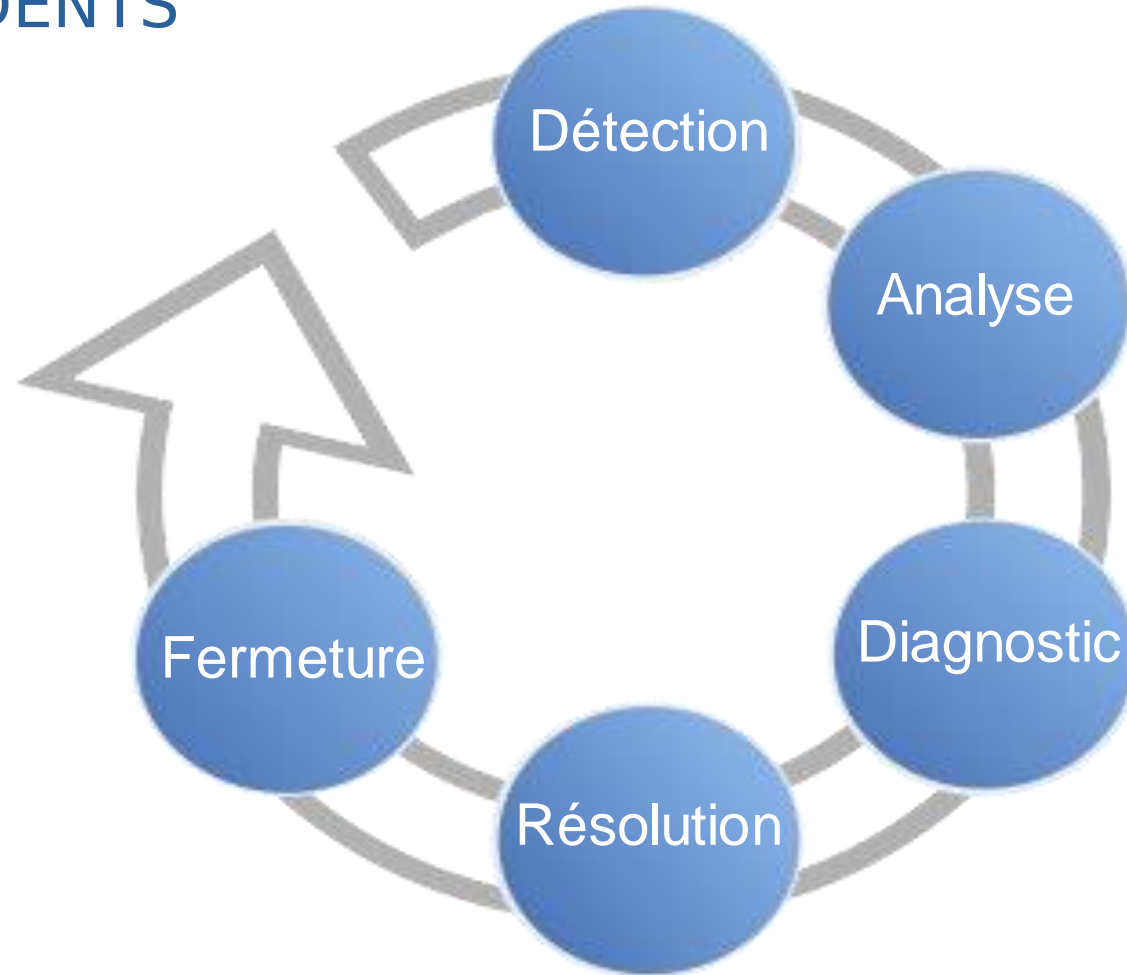
Catégorisation

Logiciel (ex : application hors service)

Matériel (ex : disque dur saturé)

Situation de départ (réf ITIL)

GESTION D'INCIDENTS



Situation de départ (réf ITIL)

KPIS DE GESTION D'INCIDENTS

Nombre d'incidents récurrents

Nombre d'incidents en suspens

Nombre total d'incidents décomptés

Temps moyen de résolution d'un incident

Etc.

PLAN

1 SITUATION DE DÉPART (Réf ITIL)

2 CHALLENGE

3 ASTUCE

4 EXEMPLE

5 BÉNÉFICES

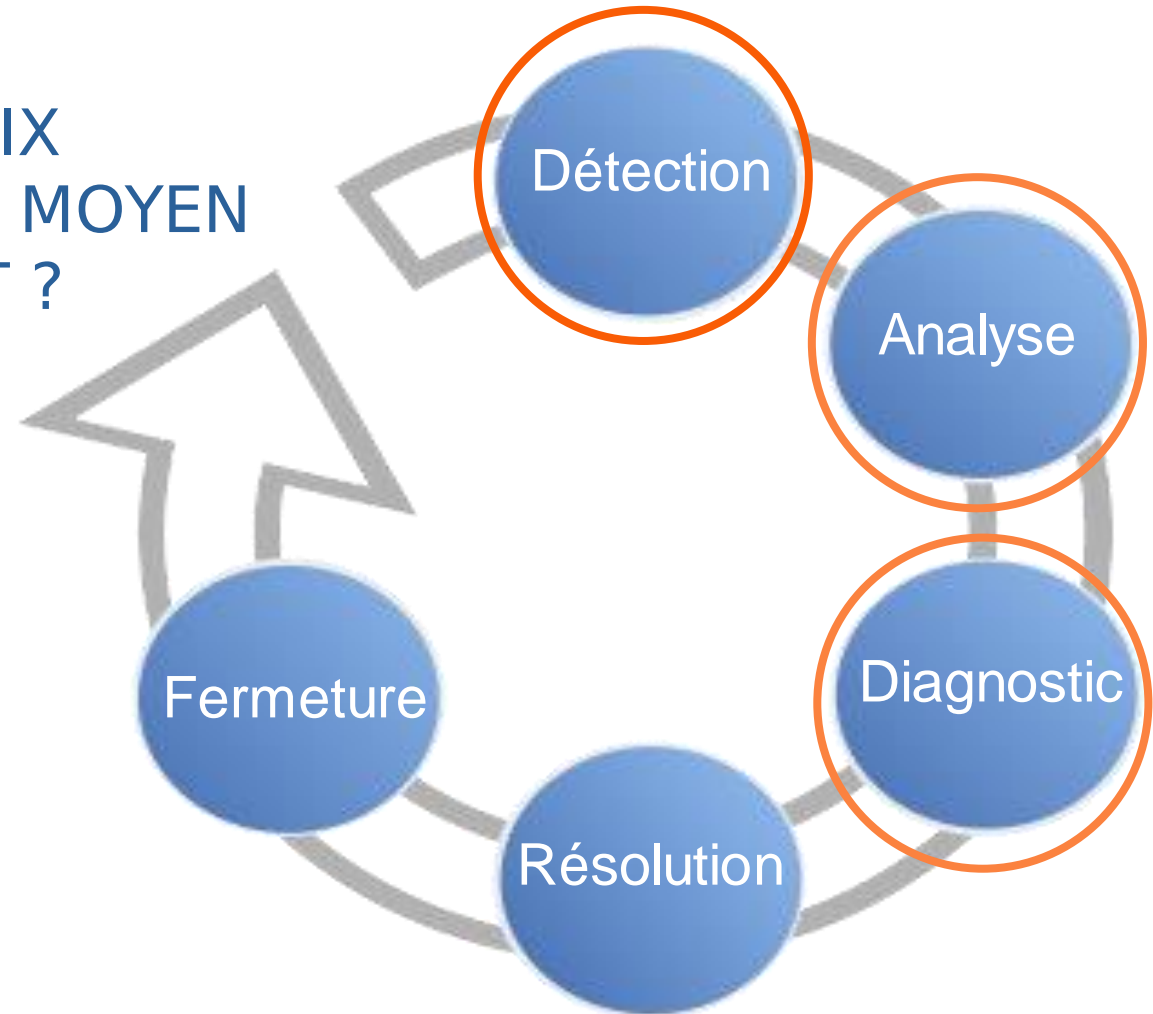
FRENCH

ZABBIX 

MEETUP ONLINE '20

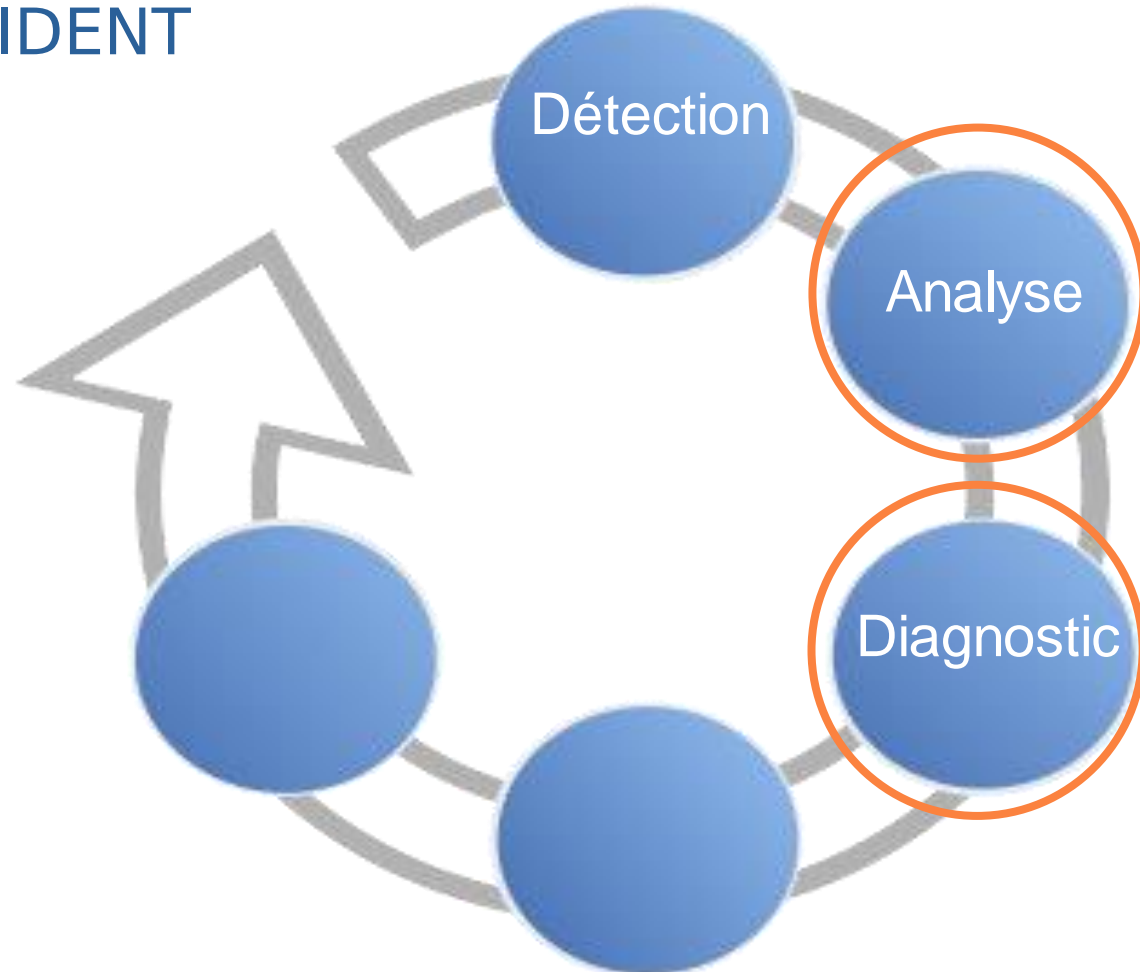
Challenge

COMMENT EXPLOITER ZABBIX
POUR OPTIMISER LE TEMPS MOYEN
DE GESTION D'UN INCIDENT ?



Challenge

LA DÉTECTION ZABBIX D'INCIDENT
EST AUTOMATIQUE



Challenge

COMMENT EXPLOITER ZABBIX POUR MINIMALISER
LE DÉLAI MOYEN D'ANALYSE ET DE DIAGNOSTIC ?

Classer

Définir l'impact et l'urgence

Révéler les symptômes complets

PLAN

1 SITUATION DE DÉPART (Réf ITIL)

2 CHALLENGE

3 ASTUCE

4 EXEMPLE

5 BÉNÉFICES

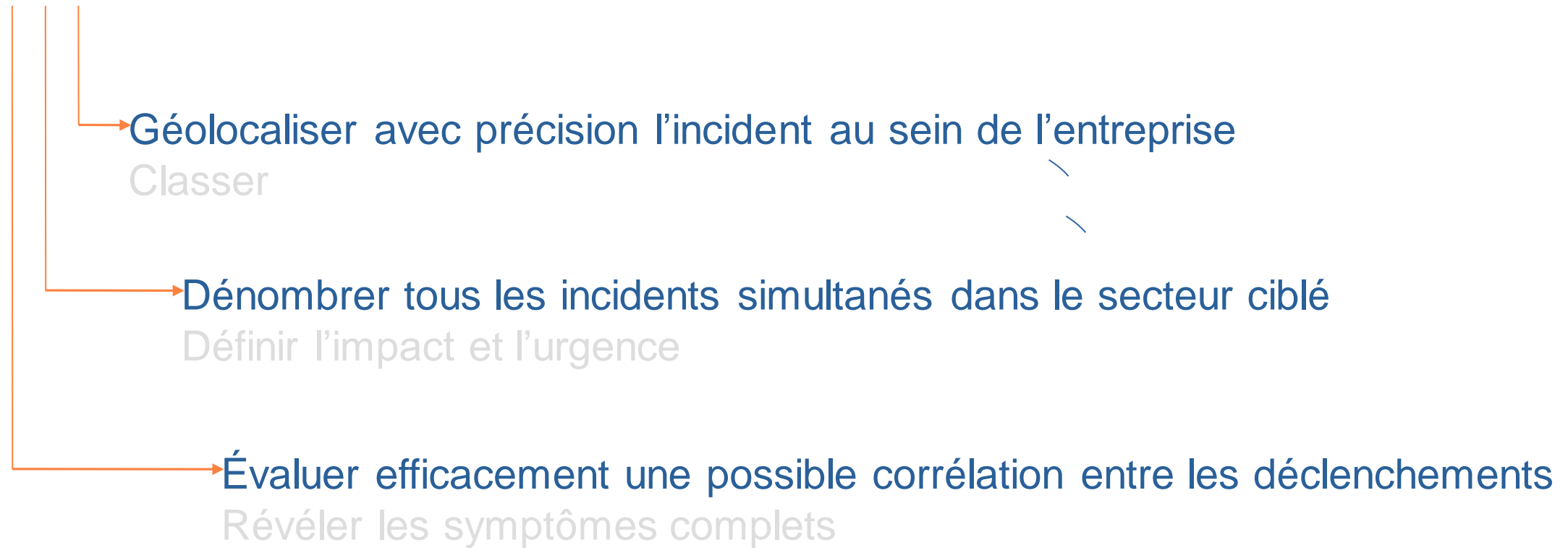
FRENCH

ZABBIX 

MEETUP ONLINE '20

Astuce

RÉCAPITULATIF DES PROCÉDURES À ACCÉLÉRER AVEC ZABBIX

- 
- Géolocaliser avec précision l'incident au sein de l'entreprise
Classer
 - Dénombrer tous les incidents simultanés dans le secteur ciblé
Définir l'impact et l'urgence
 - Évaluer efficacement une possible corrélation entre les déclenchements
Révéler les symptômes complets

Astuce

CONCEPT

→ Remplacer les fichiers d'historique d'incidents par des **cartes Zabbix** visualisées en temps réel sur les écrans de surveillance de la « tour de contrôle »

ENJEU

→ Accélérer l'analyse des informations remontées en temps en réel
La lecture d'images (carte) plus rapide que celle de table de texte (historique)

Astuce

POINT CLÉ

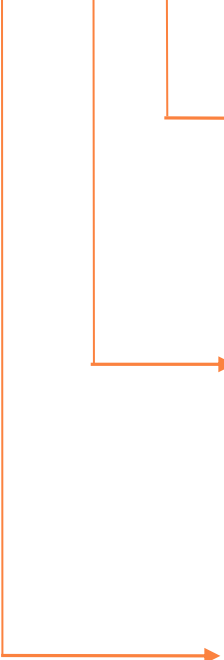
Créer des designs efficaces de cartes Zabbix

PRÉREQUIS

Connaître les métriques de surveillance du réseau de l'entreprise
Avoir une bonne sensibilité esthétique
Être utilisateur Zabbix

Astuce

PRINCIPE



Créer des cartes Zabbix de chaque secteur (étage)
conformes au plan d'architecture et à la topologie physique du réseau

Créer une carte Zabbix de synthèse
récapitulative des incidents remontés sur les cartes de secteur

Configurer des associations URL
entre cartes de « secteur » et carte de synthèse
accès utile pour les analyses approfondies et rapides

PLAN

1 SITUATION DE DÉPART (Réf ITIL)

2 CHALLENGE

3 ASTUCE

4 EXEMPLE

5 BÉNÉFICES

FRENCH

ZABBIX 

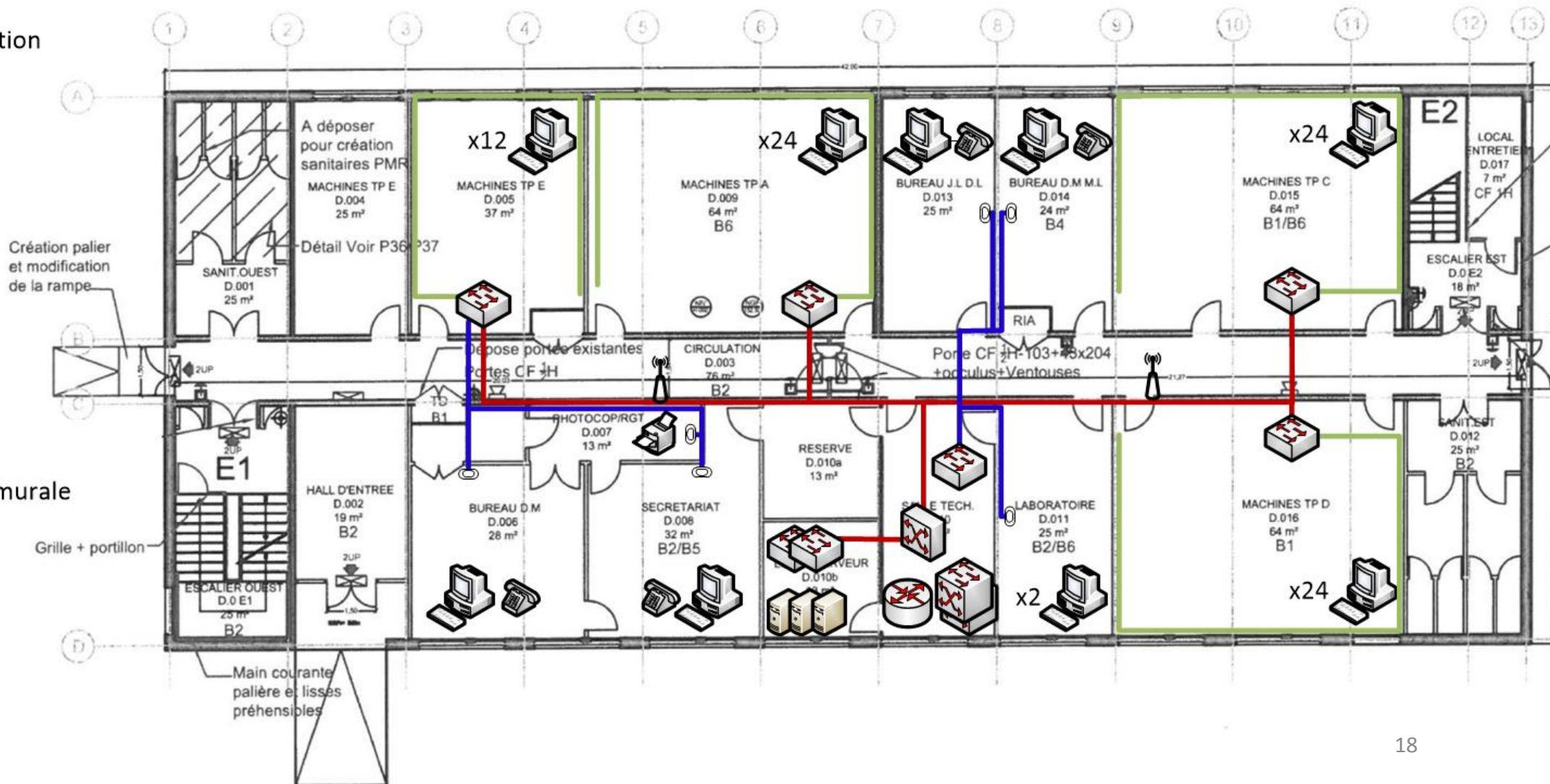
MEETUP ONLINE '20

Exemple

CAS DE SURVEILLANCE D'UN RESEAU SIMPLE

PLAN D'ARCHITECTURE

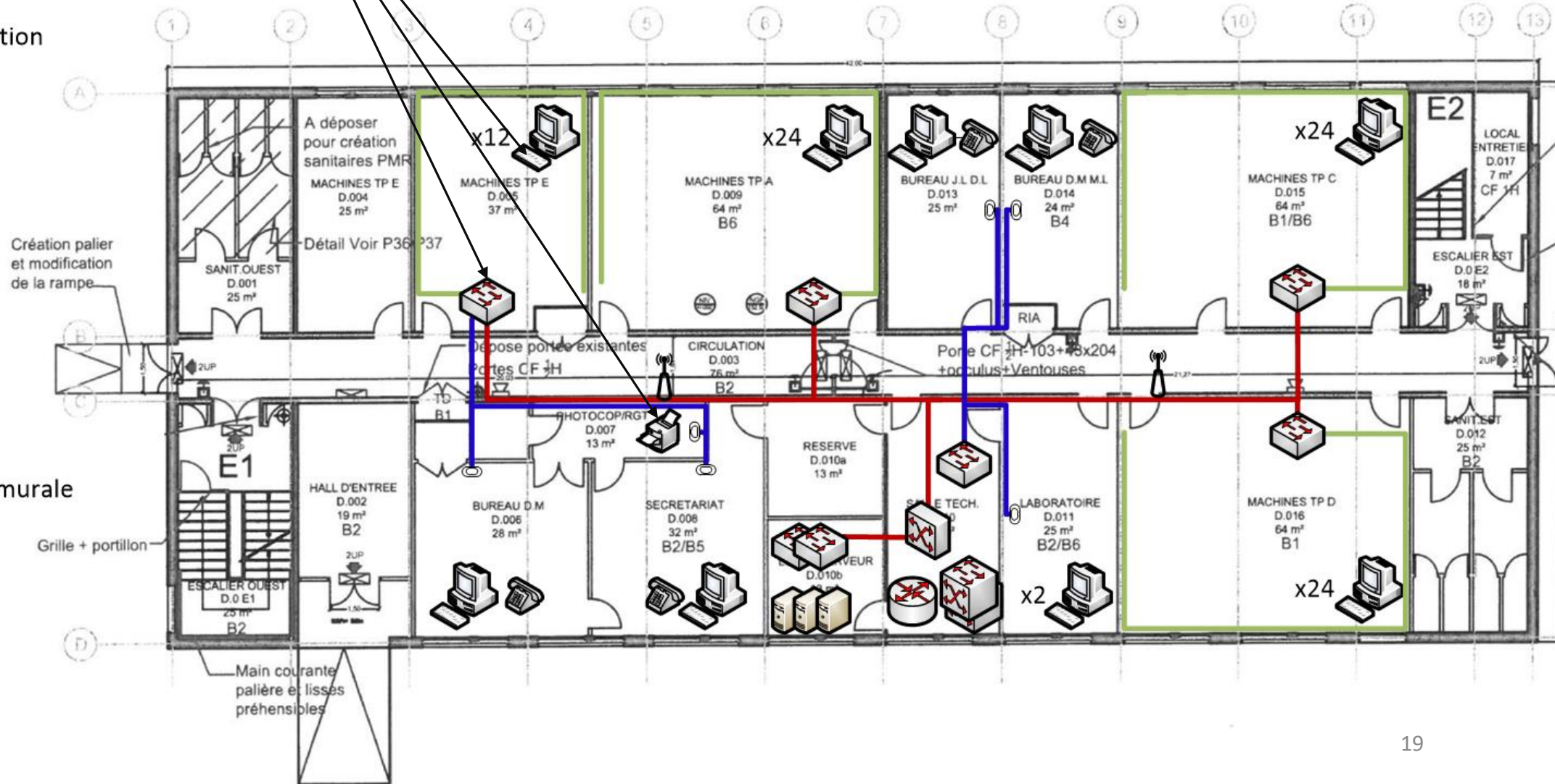
-  Switch Coeur
-  Switch de Distribution
-  Switch d'accès
-  Borne Wi-Fi
-  Serveur
-  Ordinateur
-  Téléphone
-  Prise murale
-  Liaison SW d'accès
-  Câblage des prises murale
-  Goulotte



Exemple

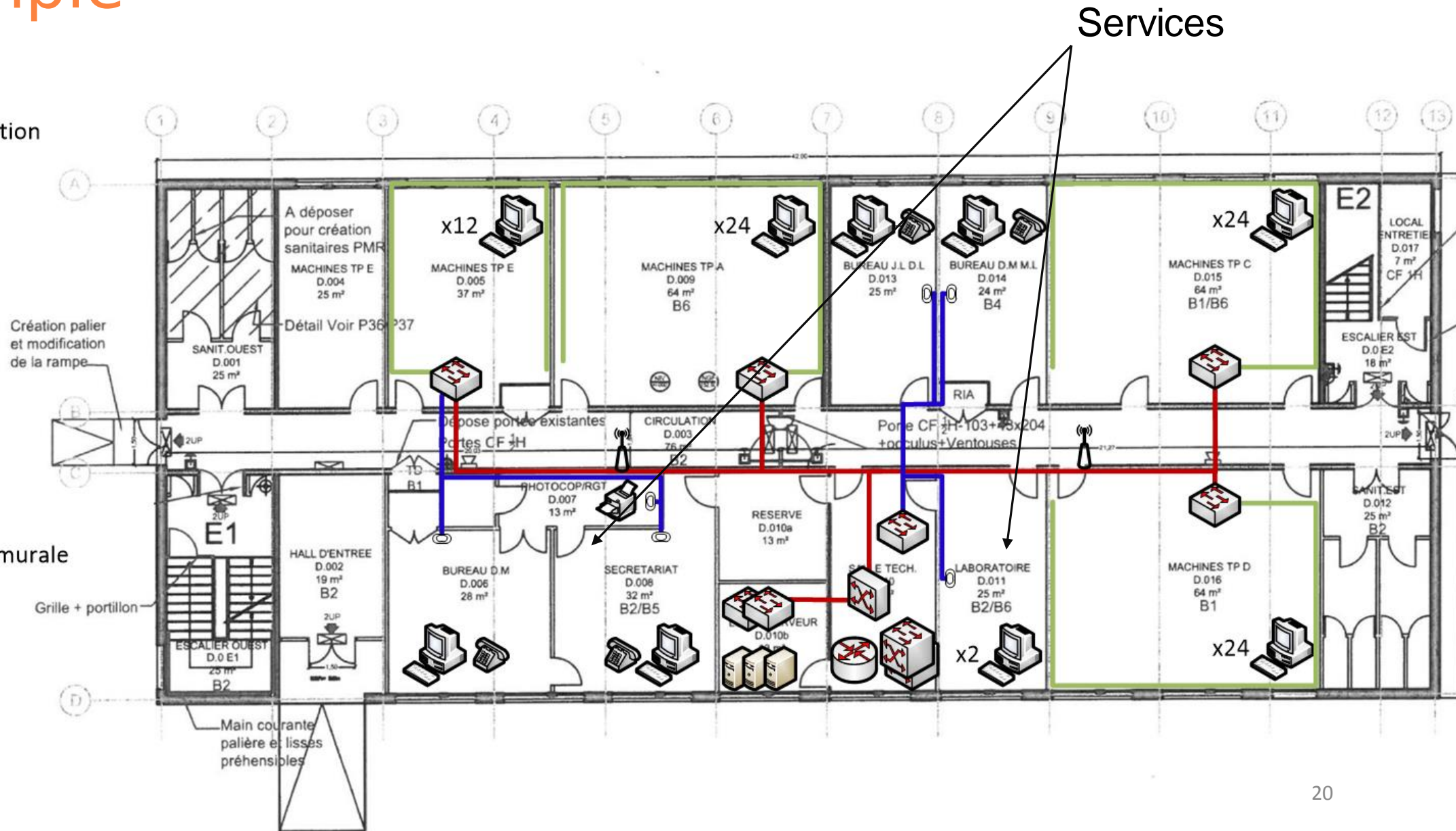
Equipements réseau

- Switch Coeur
- Switch de Distribution
- Switch d'accès
- Borne Wi-Fi
- Serveur
- Ordinateur
- Téléphone
- Prise murale
- Liaison SW d'accès
- Câblage des prises murale
- Goulotte



Exemple

-  Switch Coeur
-  Switch de Distribution
-  Switch d'accès
-  Borne Wi-Fi
-  Serveur
-  Ordinateur
-  Téléphone
-  Prise murale
-  Liaison SW d'accès
-  Câblage des prises murale
-  Goulotte



Services

Exemple

Réseau Core



Switch Coeur



Switch de Distribution



Switch d'accès



Borne Wi-Fi



Serveur



Ordinateur



Téléphone



Prise murale



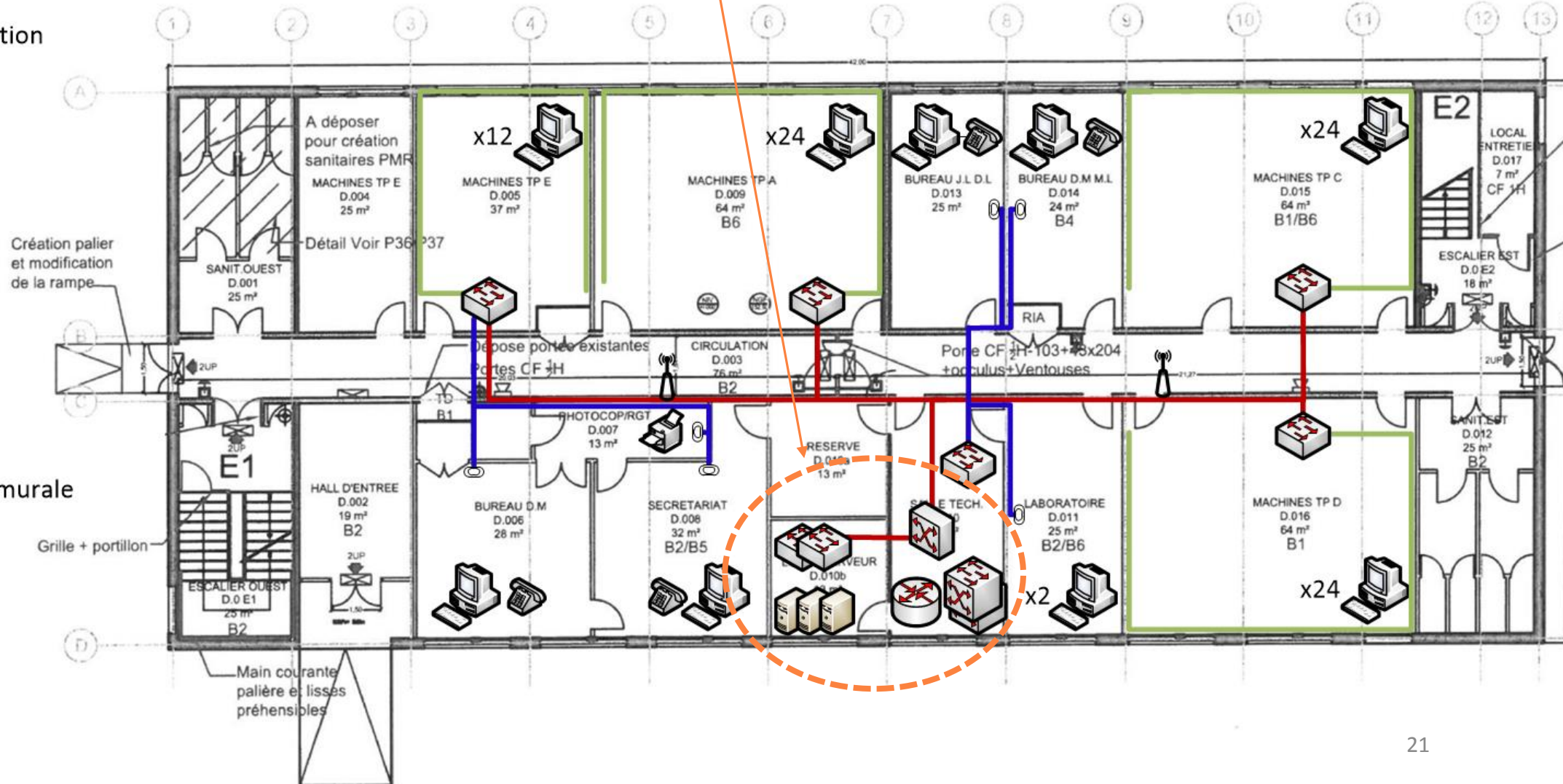
Liaison SW d'accès



Câblage des prises murale



Goulotte



Les hôtes du réseau ont été ajouté sur Zabbix

Groupes d'hotes

- Acces Point X
- camera de surveillance X
- imprimante X
- Poste de travail X
- Routeur X
- Switch Access X
- Switch Core X
- switch Distribution X
- Telephone IP X

Sélectionner

Surveillé par

- Tous
- Serveur
- Proxy

Proxy

Sélectionner

Tags

- Et/Ou
- Ou

tag

Contient

Égal

valeur

[Supprimer](#)

[Ajouter](#)

Modèles

taper ici pour rechercher

Sélectionner

Nom

DNS

IP

Port

Appliquer

Réinitialiser



Comment classer, analyser et diagnostiquer rapidement ?

Afficher les détails

Mettre en surbrillance la ligne entière

Appliquer

Réinitialiser



Temps	<input type="checkbox"/>	Sévérité	Moment de la récupération	État	Info	Hôte	Problème	Durée	Acquitté
19:12:07	<input type="checkbox"/>	Haut		PROBLÈME		PC -RDC-TPC	Unavailable by ICMP ping ?	7m 4s	Non
19:11:27	<input type="checkbox"/>	Haut		PROBLÈME		SWA RDC-TPC	Unavailable by ICMP ping ?	7m 44s	Non
19:10:19	<input type="checkbox"/>	Haut		PROBLÈME		Pr -RDC-TPC	Unavailable by ICMP ping ?	8m 52s	Non
19:07:05	<input type="checkbox"/>	Haut		PROBLÈME		PC -RDC-TPD	Unavailable by ICMP ping ?	12m 6s	Non
19:06:34	<input type="checkbox"/>	Haut		PROBLÈME		AP -RDC-Lab	Unavailable by ICMP ping ?	12m 37s	Non
19:06:31	<input type="checkbox"/>	Haut		PROBLÈME		SWA RDC-TPD	Unavailable by ICMP ping ?	12m 40s	Non
19:06:25	<input type="checkbox"/>	Haut		PROBLÈME		Cam -RDC-Ext1	Unavailable by ICMP ping ?	12m 46s	Non
19:06:25	<input type="checkbox"/>	Haut		PROBLÈME		Cam -RDC-Ext2	Unavailable by ICMP ping ?	12m 46s	Non
19:05:22	<input type="checkbox"/>	Haut		PROBLÈME		Cam -RDC-Hall	Unavailable by ICMP ping ?	13m 49s	Non
19:05:11	<input type="checkbox"/>	Haut		PROBLÈME		SWA RDC-TPE	Unavailable by ICMP ping ?	14m	Non
19:05:11	<input type="checkbox"/>	Haut		PROBLÈME		PC -RDC-TPE	Unavailable by ICMP ping ?	14m	Non
19:05:02	<input type="checkbox"/>	Haut		PROBLÈME		PC -RDC-DM	Unavailable by ICMP ping ?	14m 9s	Non
19:04:19	<input type="checkbox"/>	Haut		PROBLÈME		Pr -RDC-Sec	Unavailable by ICMP ping ?	14m 52s	Non
19:04:16	<input type="checkbox"/>	Haut		PROBLÈME		IP -RDC-Sec	Unavailable by ICMP ping ?	14m 55s	Non
19:04:14	<input type="checkbox"/>	Haut		PROBLÈME		IP -RDC-DM	Unavailable by ICMP ping ?	14m 57s	Non
19:04:05	<input type="checkbox"/>	Haut		PROBLÈME		PC -RDC-Sec	Unavailable by ICMP ping ?	15m 6s	Non

Exemple

CRÉATION DE CARTE ZABBIX DE SECTEUR (OU ÉTAGE)

CRÉATION DE CARTE ZABBIX DE SECTEUR (OU ÉTAGE)

Créer une nouvelle carte

Matérialiser le plan d'architecture dans l'éditeur de la carte

Ajouter les hôtes conformément à la topologie physique et les associer à des déclencheurs

Schématiser la connectique réelle par ajout de 'points de liaison' pour créer des bifurcations

Activer l'état des liens par association à des déclencheurs

Exemple

ZABBIX DESIGN

* Propriétaire Admin (Zabbix Administrator) X

Sélectionner

* Nom RDC Network

* Largeur 1400

* Hauteur 700

Image de fond Aucune image v

Correspondance d'icône automatique <manuel> v [afficher les correspondances d'icônes](#)

Icône surlignée

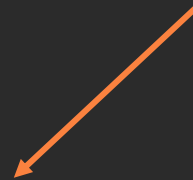
Marquer les éléments lors de changement de l'état du déclencheur

Afficher les problèmes

Détailier problème unique

Nombre de problèmes

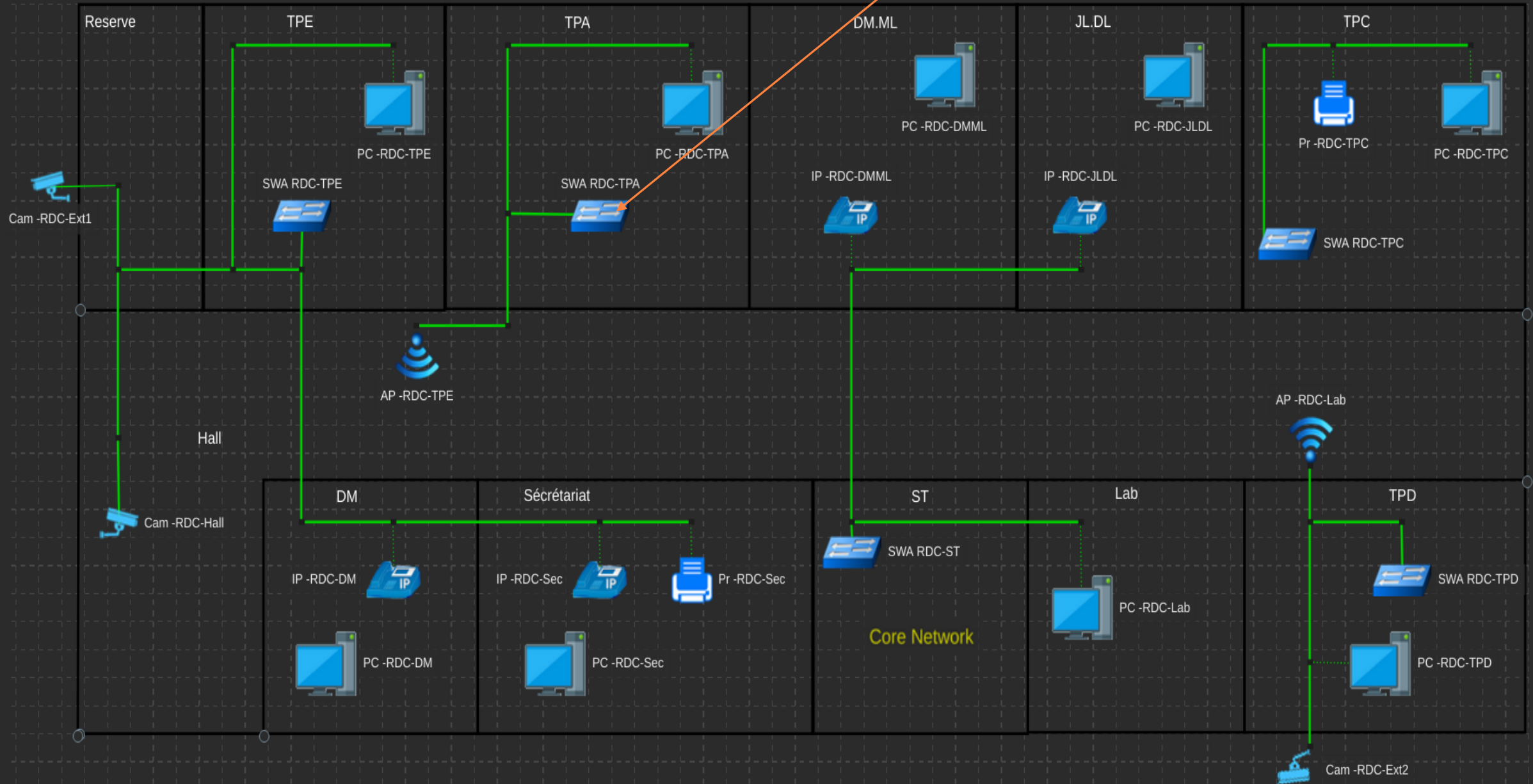
Nombre de problèmes et détailler le plus critique





{MAP.NAME}

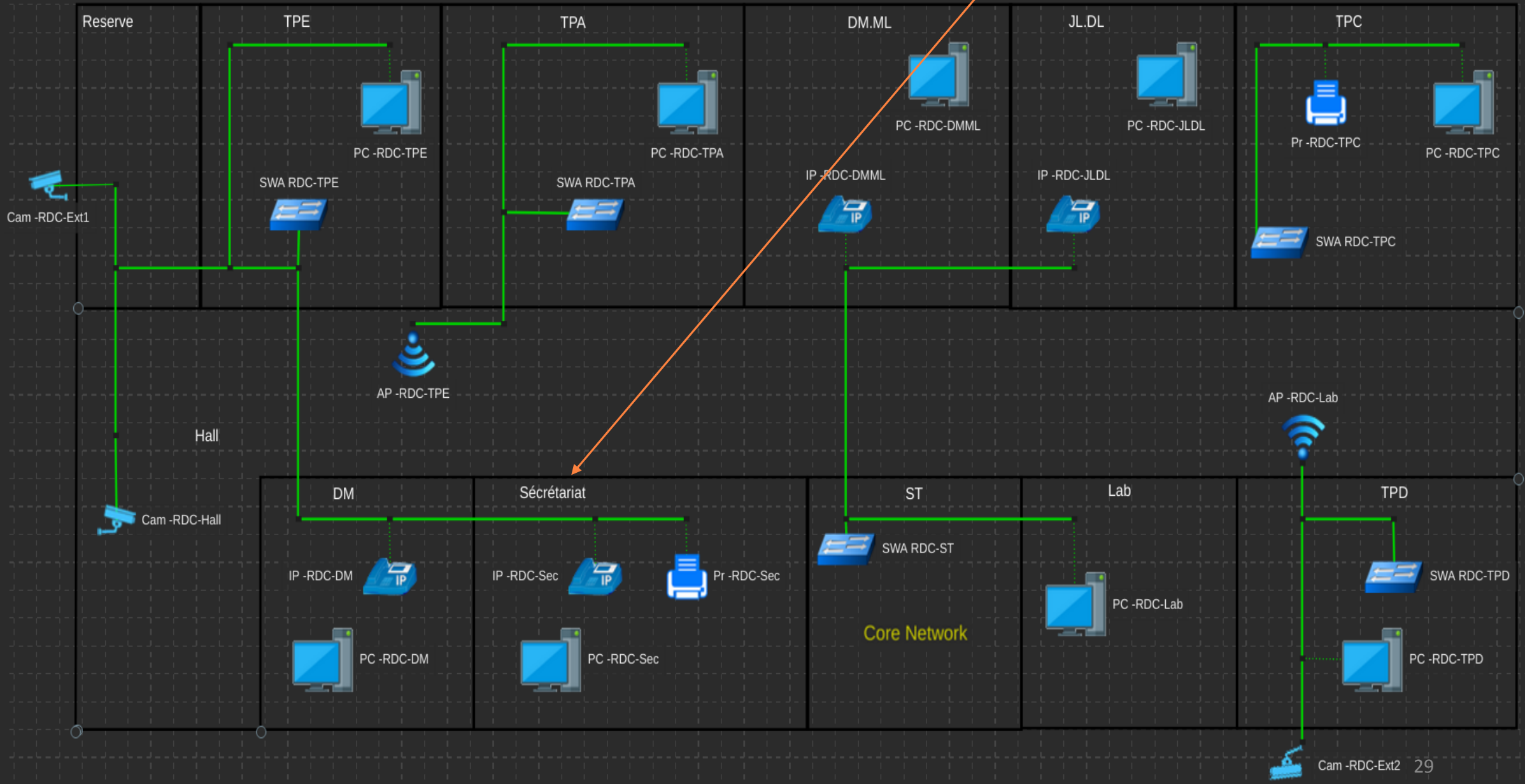
Equipement





{MAP.NAME}

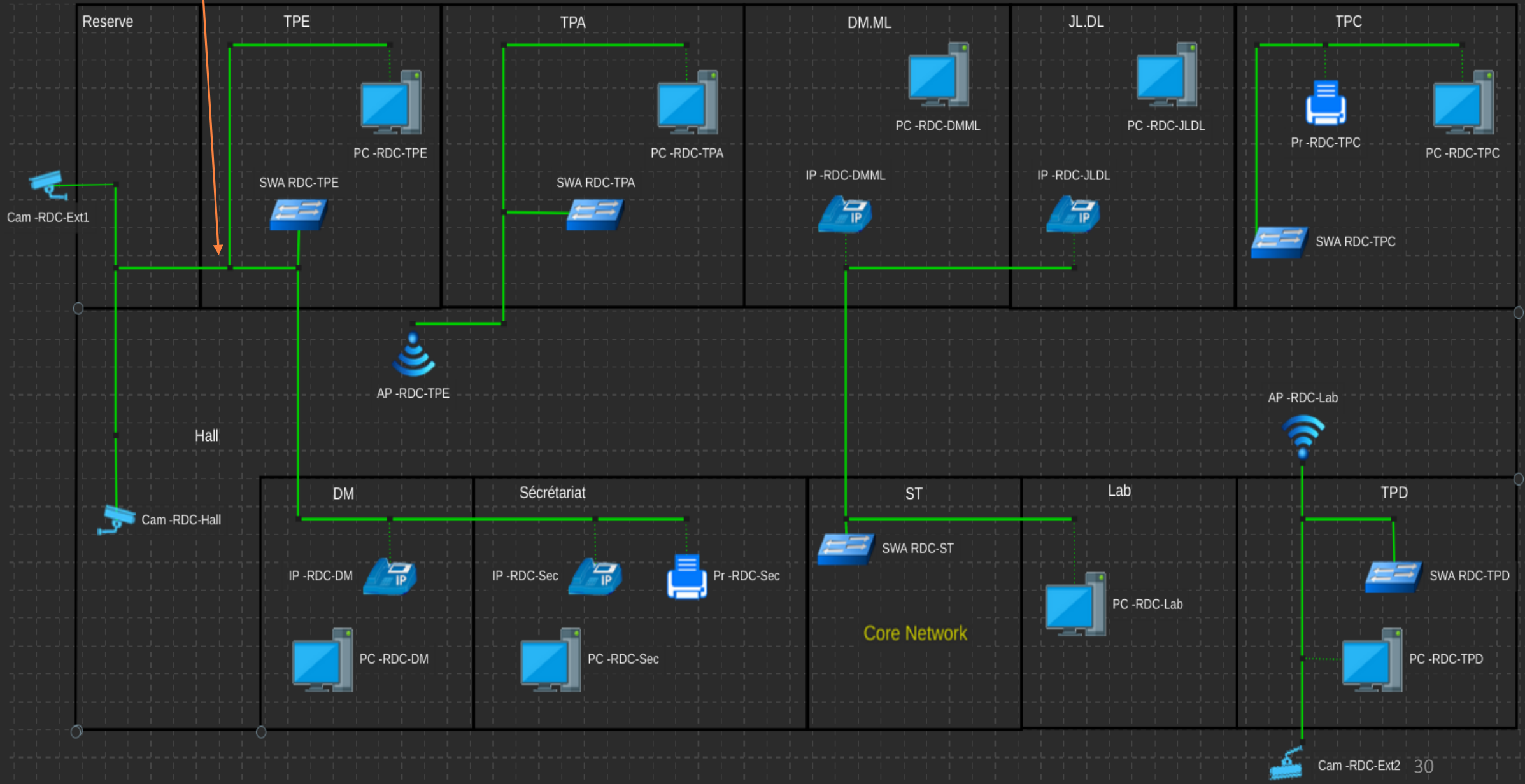
Services





Point de raccord

{MAP.NAME}



Liens

Nom de l'élément

Indicateurs de lien

Action

Point de raccord

Pr -RDC-Sec: Unavailable by ICMP ping
SWA RDC-TPE: Unavailable by ICMP ping

[Édition](#)

Étiquette


Connexion à

Point de raccord

Type (OK)

Point

Couleur (OK)

 00CC00

Indicateurs de lien

Déclencheur


Type

Couleur

Action

Pr -RDC-Sec: Unavailable by ICMP ping


Point

 DD0000

[Supprimer](#)

SWA RDC-TPE: Unavailable by ICMP ping

Point

 DD0000

[Supprimer](#)

[Ajouter](#)

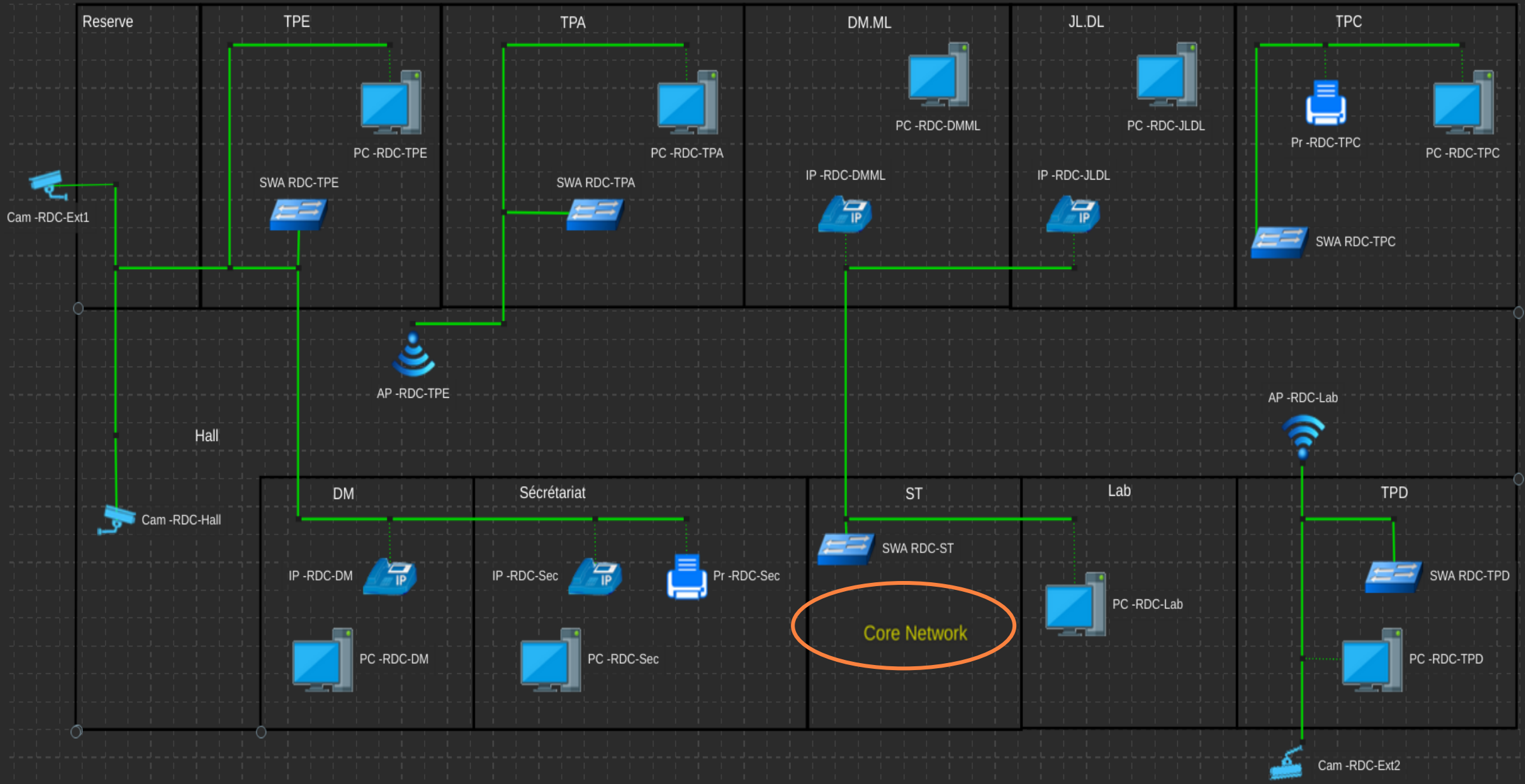
Appliquer

Supprimer

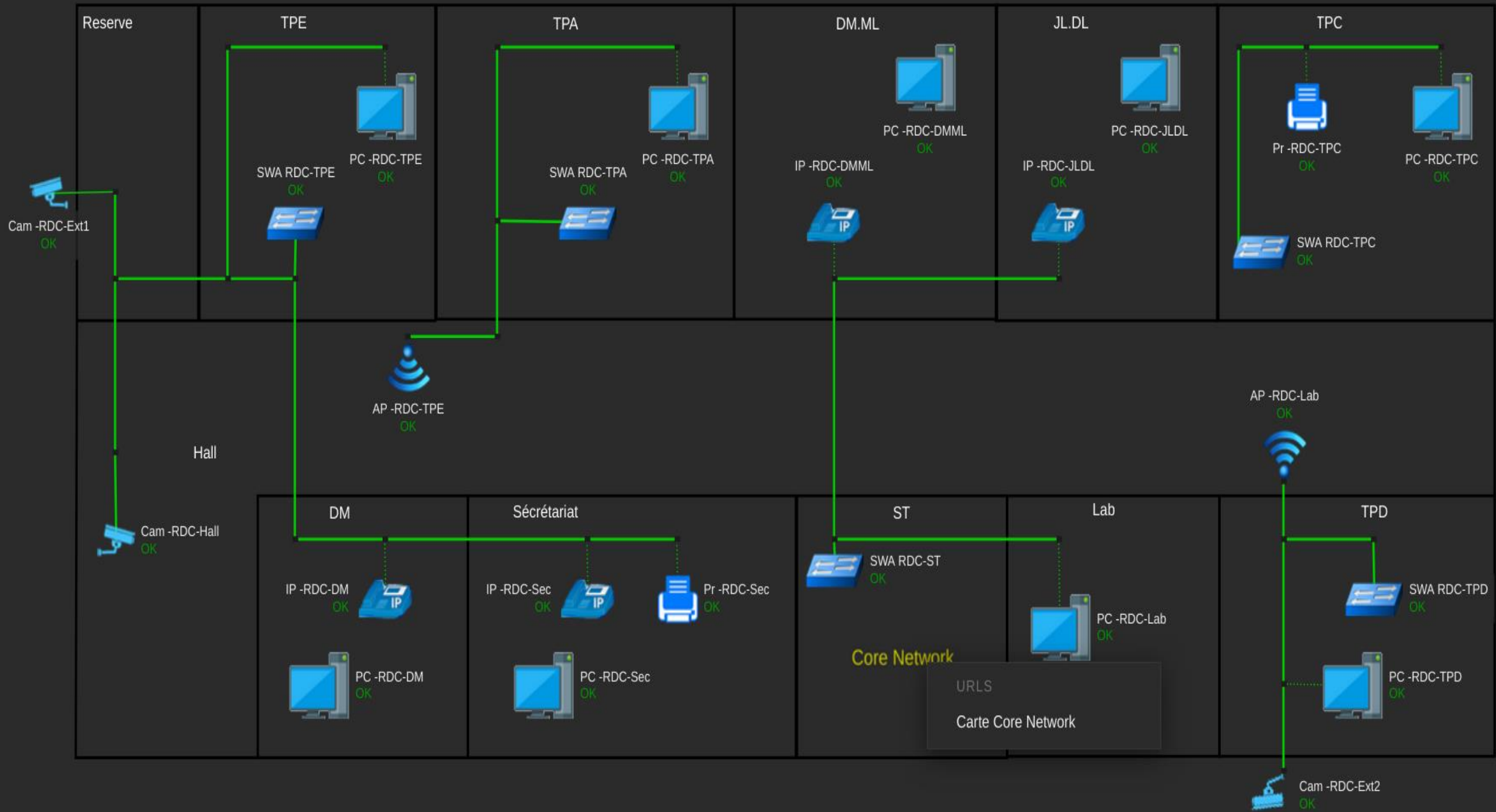
Fermer



{MAP.NAME}



RDC Network



Exemple

GESTION D'INCIDENTS

Afficher les détails

Mettre en surbrillance la ligne entière

Appliquer

Réinitialiser

Temps	Sévérité	Moment de la récupération	État	Info	Hôte	Problème	Durée	Acquitté
19:12:07	Haut		PROBLÈME		PC -RDC-TPC	Unavailable by ICMP ping ?	7m 4s	Non
19:11:27	Haut		PROBLÈME		SWA RDC-TPC	Unavailable by ICMP ping ?	7m 44s	Non
19:10:19	Haut		PROBLÈME		Pr -RDC-TPC	Unavailable by ICMP ping ?	8m 52s	Non
19:07:05	Haut		PROBLÈME		PC -RDC-TPD	Unavailable by ICMP ping ?	12m 6s	Non
19:06:34	Haut		PROBLÈME		AP -RDC-Lab	Unavailable by ICMP ping ?	12m 37s	Non
19:06:31	Haut		PROBLÈME		SWA RDC-TPD	Unavailable by ICMP ping ?	12m 40s	Non
19:06:25	Haut		PROBLÈME		Cam -RDC-Ext1	Unavailable by ICMP ping ?	12m 46s	Non
19:06:25	Haut		PROBLÈME		Cam -RDC-Ext2	Unavailable by ICMP ping ?	12m 46s	Non
19:05:22	Haut		PROBLÈME		Cam -RDC-Hall	Unavailable by ICMP ping ?	13m 49s	Non
19:05:11	Haut		PROBLÈME		SWA RDC-TPE	Unavailable by ICMP ping ?	14m	Non
19:05:11	Haut		PROBLÈME		PC -RDC-TPE	Unavailable by ICMP ping ?	14m	Non
19:05:02	Haut		PROBLÈME		PC -RDC-DM	Unavailable by ICMP ping ?	14m 9s	Non
19:04:19	Haut		PROBLÈME		Pr -RDC-Sec	Unavailable by ICMP ping ?	14m 52s	Non
19:04:16	Haut		PROBLÈME		IP -RDC-Sec	Unavailable by ICMP ping ?	14m 55s	Non
19:04:14	Haut		PROBLÈME		IP -RDC-DM	Unavailable by ICMP ping ?	14m 57s	Non
19:04:05	Haut		PROBLÈME		PC -RDC-Sec	Unavailable by ICMP ping ?	15m 6s	Non

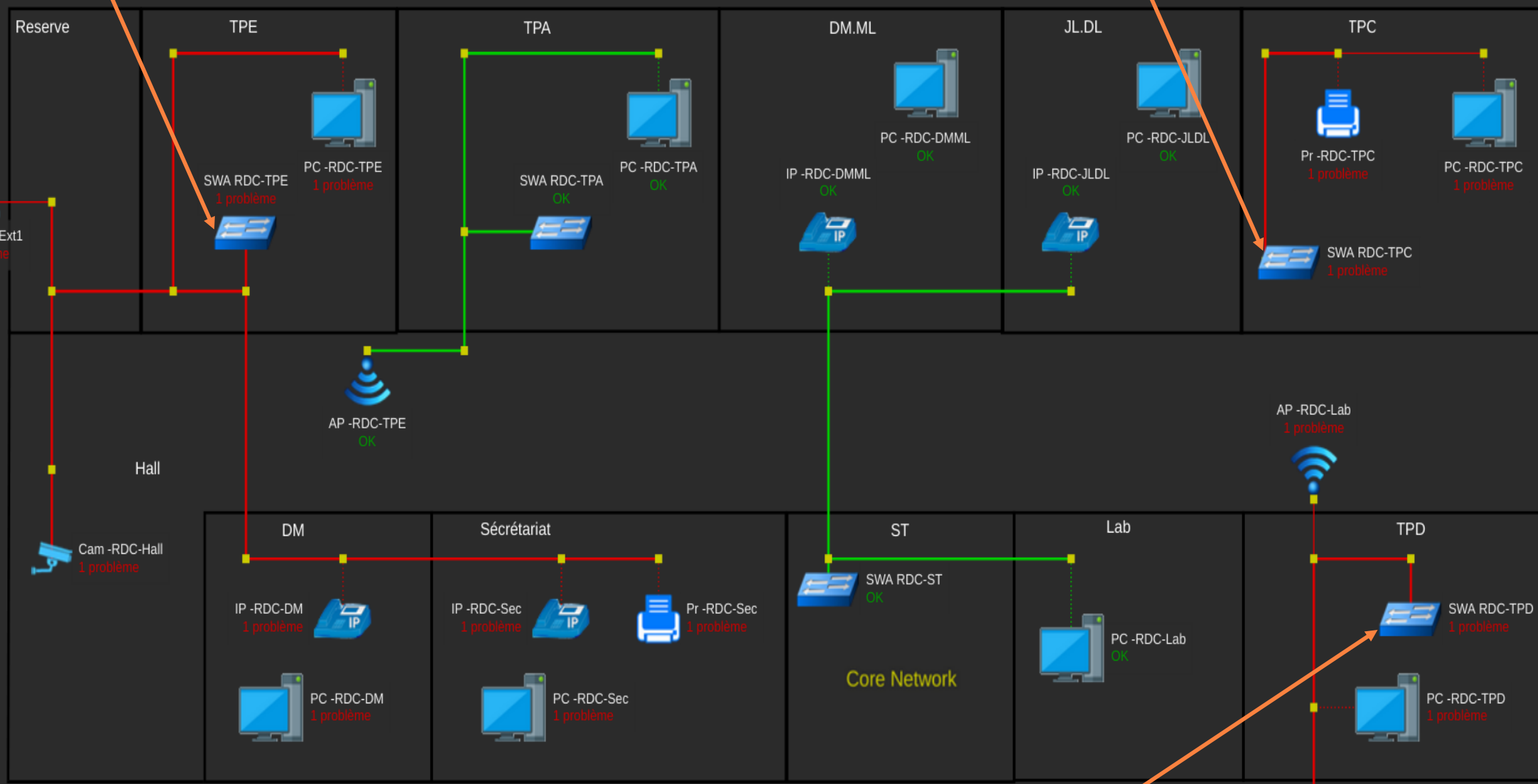


Probable source de l'incident

RDC Network

Probable source de l'incident

Probable source de l'incident



Exemple

CAS DE SURVEILLANCE D'UN RESEAU « MOINS » SIMPLE
(bâtiment à plusieurs niveaux)



21:13:51	Haut	PROBLÈME	PC -N1-Lab	Unavailable by ICMP ping	3m 50s	Non
21:13:48	Haut	PROBLÈME	PC -N1-JLDL	Unavailable by ICMP ping	3m 53s	Non
21:12:45	Haut	PROBLÈME	PC -N1-DMML	Unavailable by ICMP ping	4m 56s	Non
21:12:18	Haut	PROBLÈME	IF -N1-JLDL	Unavailable by ICMP ping	5m 23s	Non
21:12:15	Haut	PROBLÈME	IP -N1-DMML	Unavailable by ICMP ping	5m 26s	Non
21:12:01	Haut	PROBLÈME	SWA N1-ST	Unavailable by ICMP ping	5m 40s	Non
21:09:54	Haut	PROBLÈME	PC -N2-TPA	Unavailable by ICMP ping	7m 47s	Non
21:09:42	Haut	PROBLÈME	AP -N2-TPE	Unavailable by ICMP ping	7m 59s	Non
21:09:05	Haut	PROBLÈME	SWA N2-TPA	Unavailable by ICMP ping	8m 36s	Non
21:00						
19:12:07	Haut	PROBLÈME	PC -RDC-TPC	Unavailable by ICMP ping	2h 5m 34s	Non
19:11:27	Haut	PROBLÈME	SWA RDC-TPC	Unavailable by ICMP ping	2h 6m 14s	Non
19:10:19	Haut	PROBLÈME	Pr -RDC-TPC	Unavailable by ICMP ping	2h 7m 22s	Non
19:07:05	Haut	PROBLÈME	PC -RDC-TPD	Unavailable by ICMP ping	2h 10m 36s	Non
19:06:34	Haut	PROBLÈME	AP -RDC-Lab	Unavailable by ICMP ping	2h 11m 7s	Non
19:06:31	Haut	PROBLÈME	SWA RDC-TPD	Unavailable by ICMP ping	2h 11m 10s	Non
19:06:25	Haut	PROBLÈME	Cam -RDC-Ext1	Unavailable by ICMP ping	2h 11m 16s	Non
19:06:25	Haut	PROBLÈME	Cam -RDC-Ext2	Unavailable by ICMP ping	2h 11m 16s	Non
19:05:22	Haut	PROBLÈME	Cam -RDC-Hall	Unavailable by ICMP ping	2h 12m 19s	Non
19:05:11	Haut	PROBLÈME	SWA RDC-TPE	Unavailable by ICMP ping	2h 12m 30s	Non
19:05:11	Haut	PROBLÈME	PC -RDC-TPE	Unavailable by ICMP ping	2h 12m 30s	Non
19:05:02	Haut	PROBLÈME	PC -RDC-DM	Unavailable by ICMP ping	2h 12m 39s	Non
19:04:19	Haut	PROBLÈME	Pr -RDC-Sec	Unavailable by ICMP ping	2h 13m 22s	Non

Exemple

CRÉATION DE CARTE DE SYNTHÈSE

CRÉATION DE CARTE DE SYNTHÈSE

Créer une nouvelle carte



Matérialiser le plan de secteurs dans l'éditeur de la carte



Ajouter les hôtes du réseau core conformément à la topologie physique et les associer à des déclencheurs



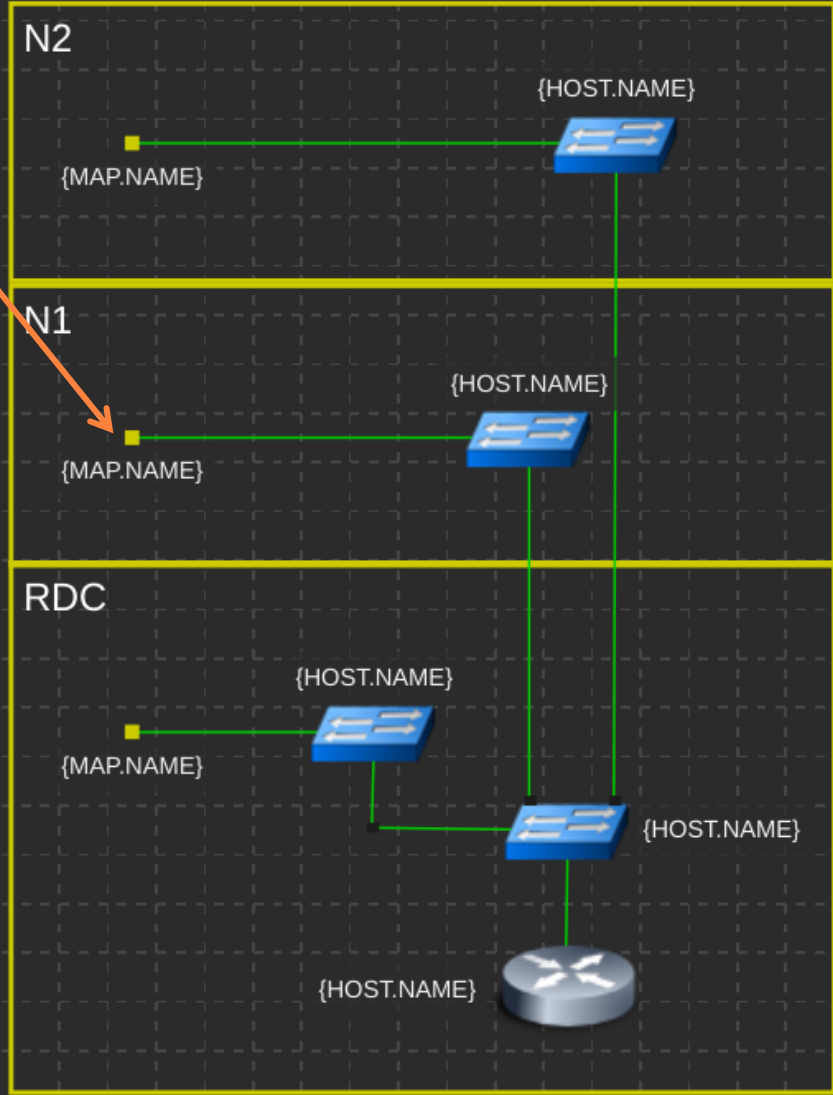
Ajouter par secteur une icône et l'associer au type d'élément 'carte'
Pour afficher le récapitulatif automatique d'incidents par secteur

Exemple

ZABBIX DESIGN

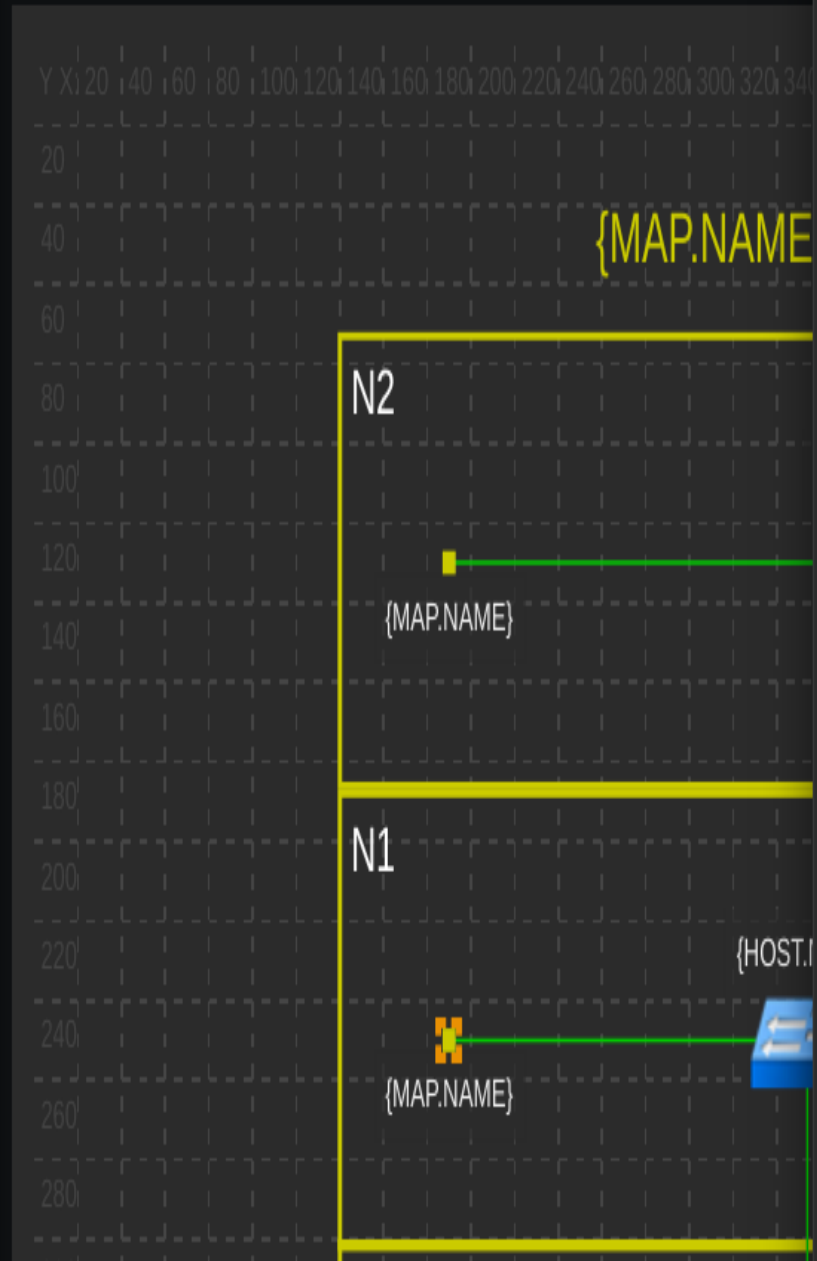
Point récapitulatif d'incidents par niveau

{MAP.NAME}





Élément de carte: [Ajouter](#) / [Supprimer](#) Forme: [Ajouter](#) / [Supprimer](#) Li



Élément de carte

Type Carte



Étiquette {MAP.NAME}

Positionnement de l'étiquette

* Carte N1 Network

Sélectionner

Icônes

Défaut

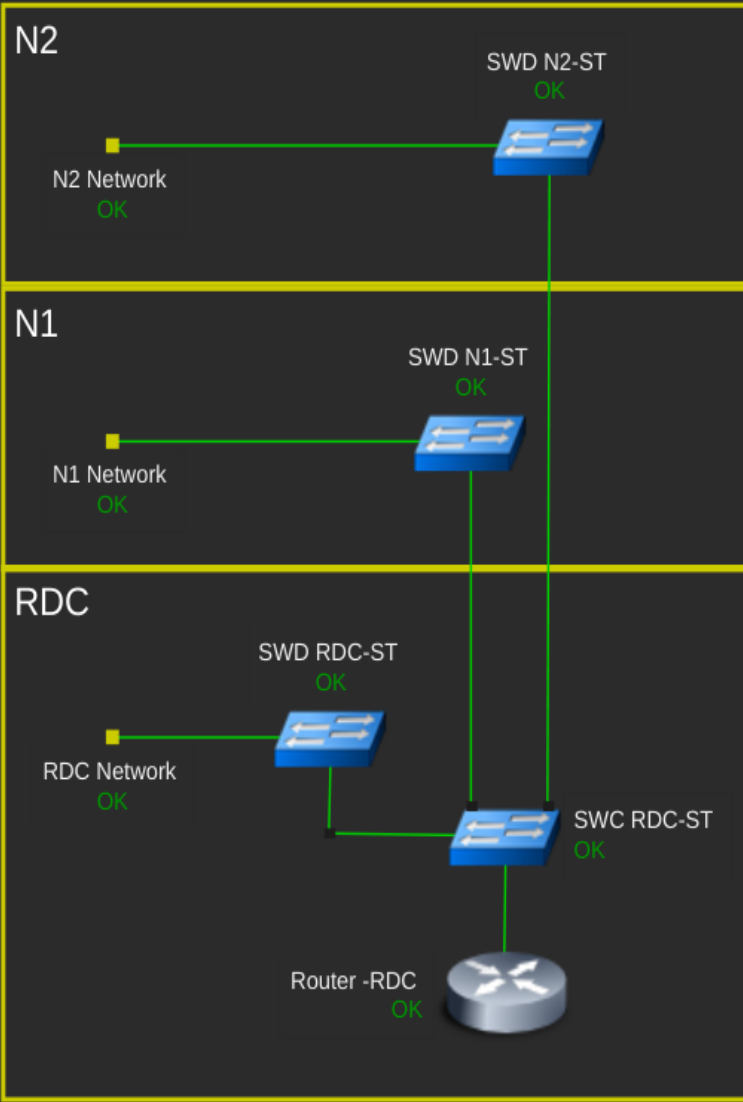
Problème

Maintenance

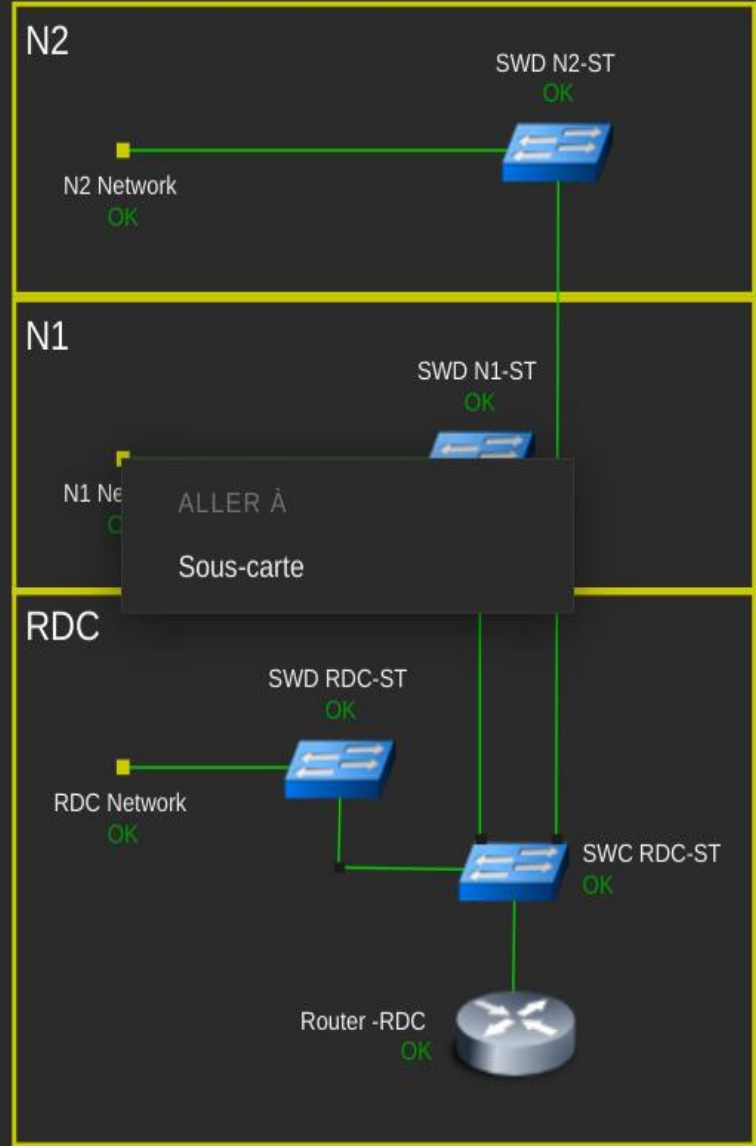
Désactivé



Core Network



Core Network



Exemple

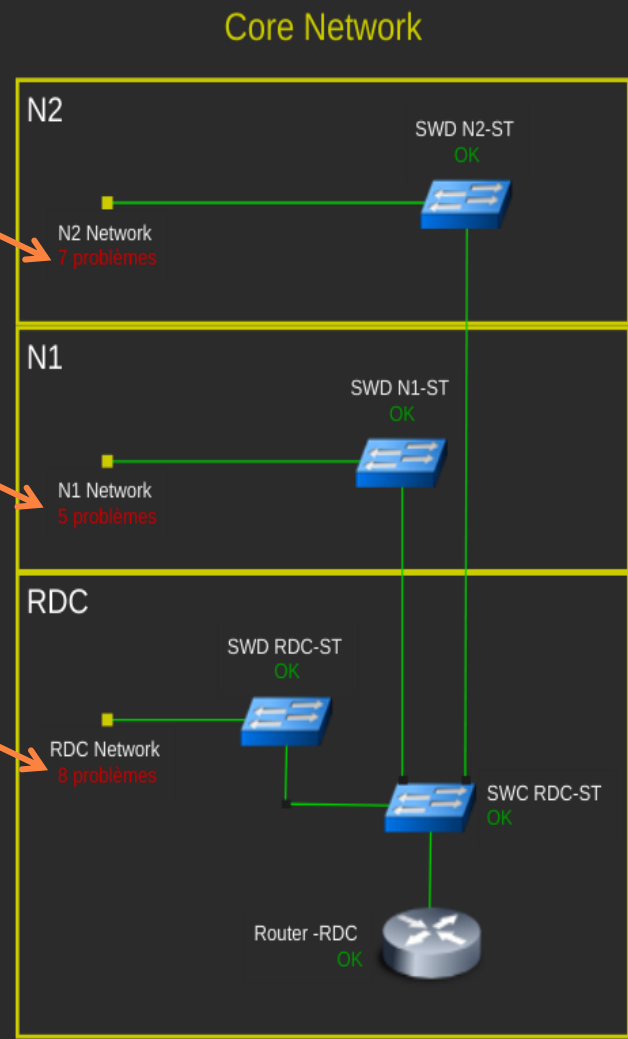
GESTION D'INCIDENTS

Navigation icons: Home, Search, Eye, List, Bar Chart, Wrench, Gear, Headphones, Z, Question Mark, Profile, Power.

21:13:51	<input type="checkbox"/>	Haut	PROBLÈME	PC -N1-Lab	↑ Unavailable by ICMP ping ?	3m 50s	Non
21:13:48	<input type="checkbox"/>	Haut	PROBLÈME	PC -N1-JLDL	↑ Unavailable by ICMP ping ?	3m 53s	Non
21:12:45	<input type="checkbox"/>	Haut	PROBLÈME	PC -N1-DMML	↑ Unavailable by ICMP ping ?	4m 56s	Non
21:12:18	<input type="checkbox"/>	Haut	PROBLÈME	IP -N1-JLDL	↑ Unavailable by ICMP ping ?	5m 23s	Non
21:12:15	<input type="checkbox"/>	Haut	PROBLÈME	IP -N1-DMML	↑ Unavailable by ICMP ping ?	5m 26s	Non
21:12:01	<input type="checkbox"/>	Haut	PROBLÈME	SWA N1-ST	↑ Unavailable by ICMP ping ?	5m 40s	Non
21:09:54	<input type="checkbox"/>	Haut	PROBLÈME	PC -N2-TPA	↑ Unavailable by ICMP ping ?	7m 47s	Non
21:09:42	<input type="checkbox"/>	Haut	PROBLÈME	AP -N2-TPE	↑ Unavailable by ICMP ping ?	7m 59s	Non
21:09:05	<input type="checkbox"/>	Haut	PROBLÈME	SWA N2-TPA	↑ Unavailable by ICMP ping ?	8m 36s	Non
21:00	<input type="radio"/>						
19:12:07	<input type="checkbox"/>	Haut	PROBLÈME	PC -RDC-TPC	↑ Unavailable by ICMP ping ?	2h 5m 34s	Non
19:11:27	<input type="checkbox"/>	Haut	PROBLÈME	SWA RDC-TPC	↑ Unavailable by ICMP ping ?	2h 6m 14s	Non
19:10:19	<input type="checkbox"/>	Haut	PROBLÈME	Pr -RDC-TPC	↑ Unavailable by ICMP ping ?	2h 7m 22s	Non
19:07:05	<input type="checkbox"/>	Haut	PROBLÈME	PC -RDC-TPD	↑ Unavailable by ICMP ping ?	2h 10m 36s	Non
19:06:34	<input type="checkbox"/>	Haut	PROBLÈME	AP -RDC-Lab	↑ Unavailable by ICMP ping ?	2h 11m 7s	Non
19:06:31	<input type="checkbox"/>	Haut	PROBLÈME	SWA RDC-TPD	↑ Unavailable by ICMP ping ?	2h 11m 10s	Non
19:06:25	<input type="checkbox"/>	Haut	PROBLÈME	Cam -RDC-Ext1	↑ Unavailable by ICMP ping ?	2h 11m 16s	Non
19:06:25	<input type="checkbox"/>	Haut	PROBLÈME	Cam -RDC-Ext2	↑ Unavailable by ICMP ping ?	2h 11m 16s	Non
19:05:22	<input type="checkbox"/>	Haut	PROBLÈME	Cam -RDC-Hall	↑ Unavailable by ICMP ping ?	2h 12m 19s	Non
19:05:11	<input type="checkbox"/>	Haut	PROBLÈME	SWA RDC-TPE	↑ Unavailable by ICMP ping ?	2h 12m 30s	Non
19:05:11	<input type="checkbox"/>	Haut	PROBLÈME	PC -RDC-TPE	↑ Unavailable by ICMP ping ?	2h 12m 30s	Non
19:05:02	<input type="checkbox"/>	Haut	PROBLÈME	PC -RDC-DM	↑ Unavailable by ICMP ping ?	2h 12m 39s	Non
19:04:19	<input type="checkbox"/>	Haut	PROBLÈME	Pr -RDC-Sec	↑ Unavailable by ICMP ping ?	2h 13m 22s	Non

Problème sur Pr -N1-TPC
Unavailable by ICMP ping
14/09/2020 17:37:38

Analyse rapide d'incidents par niveau



PLAN

1 SITUATION DE DÉPART (Réf ITIL)

2 CHALLENGE

3 ASTUCE

4 EXEMPLE

5 BÉNÉFICES

FRENCH

ZABBIX 

MEETUP ONLINE '20

Bénéfices

Délai réduit de ~ 50%
en gestion d'incident (réf ITIL)

Disponibilité améliorée
des services de l'entreprise

Efficacité augmentée
des communications avec l'utilisateur final

Temps libre et « ordinaire » créé
pour s'investir dans la gestion des problèmes

FRENCH

ZABBIX 

MEETUP ONLINE '20

Merci