h e g

Haute école de gestion
Genève

Conception et Développement Expérimental d'un Protocole de Gestion d'Urgence Décentralisé

Travail de Bachelor réalisé en vue de l'obtention du Bachelor HES

par :

Jean-Pierre GROSSGLAUSER

Conseiller au travail de Bachelor :

Dr Michel DERIAZ, Professeur HES

Genève, le 16 août 2024

Haute École de Gestion de Genève (HEG-GE)

Filière Informatique de Gestion

Hes·so GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre Bachelor of Science HES-SO en

Informatique de gestion.

L'étudiant a envoyé ce document par email à l'adresse remise par son directeur de mémoire afin qu'il l'analyse à l'aide du logiciel de détection de plagiat COMPILATIO.

L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 16 août 2024

Jean-Pierre Grossglauser

Remerciements

Mes remerciements vont en premier lieu à ma mère, Maria Lucia Grossglauser, pour sa fidélité, son dévouement, son soutien inconditionnel et indéfectible, ainsi qu'à mes proches.

Je remercie également tous ceux qui ont contribué favorablement à la réalisation de ce travail, en particulier le Dr Michel Deriaz, pour avoir proposé ses conseils et sa supervision ainsi que Madame Chrystel Dayer pour ses enseignements et sa bienveillance.

Enfin, je tiens aussi à remercier les personnes remarquables que j'ai eu le privilège de rencontrer au cours des dernières années, qui m'ont inspiré et permis de compléter cette formation : Monsieur Marc-Henri Jaunin; Madame Virginie Vuagniaux et Olivier Bourgeois (Fastnet SA), Madame la directrice Brigitte Bachelard et le Dr Cédric Baudet (Haute école Arc), Monsieur Franck Tournier (Université de Lausanne), Monsieur Max Andersen (Red Hat), le Brigadier Daniel Berger (Armée suisse) ainsi que le Pasteur David Valdez et sa famille.

Ce mémoire est dédié à mon père Hans Grossglauser (1942-2020).

Résumé

La gestion des situations d'urgence, qu'il s'agisse d'événements mineurs ou de crises majeures telles que les phénomènes météorologiques extrêmes, les pandémies ou les conflits armés, nécessite que chaque individu soit préparé à faire face à de telles crises en s'appuyant sur une approche décentralisée et digitalisée favorisant l'autonomie et la prise de décision collaborative. Ce mémoire propose une première version du protocole de communication de gestion d'urgence décentralisé DEMP (Decentralized Emergency Management Protocol), dont le but est d'assurer la connectivité, la réactivité et l'interopérabilité des systèmes d'information lors des situations d'urgence. Il est accompagné du prototype d'application de sécurité personnelle OASIS (Open Alert and Safety Information System), une implémentation expérimentale du protocole faisant office de preuve de concept et dont l'objectif est de permettre à chaque individu et organisation de bénéficier collectivement d'un processus d'alerte d'urgence, de partage d'informations et de suivi en temps réel.

Table des matières

Liste des tableaux

Liste des figures

1. Introduction

Les situations d'urgence, qu'elles soient d'origine naturelle, accidentelle ou intentionnelle, peuvent survenir à tout moment et exigent une réponse immédiate et efficace afin de minimiser les impacts humains et matériels. Pour améliorer la gestion d'urgence, et en particulier celle des premiers intervenants, souvent des personnes ordinaires présentes sur les lieux, il est nécessaire de repenser les systèmes actuels, traditionnellement centralisés et caractérisés par des structures hiérarchiques et des processus décisionnels pouvant être particulièrement problématiques. De plus, dans une ère où la connectivité est omniprésente, il faut pouvoir tirer pleinement parti des nouvelles technologies en termes de collecte, analyse et partage de données.

À cet égard, une approche décentralisée et digitalisée de la gestion des situations d'urgence, axée en premier lieu sur la personne et l'aspect communautaire, constitue une solution innovante et adaptée à une variété de situations d'urgence, des plus ordinaires aux plus complexes. En permettant aux citoyens d'intervenir immédiatement, en amont ou avec les services d'urgence, de nombreuses vies peuvent être préservées et des situations résolues plus efficacement. En outre, sur le plan organisationnel, cela contribuerait à améliorer les interactions entre les différents acteurs institutionnels et privés tout en permettant une allocation plus efficiente des ressources, en particulier lors de crises de grande ampleur.

Ce mémoire vise à concevoir et à développer un protocole de communication de gestion d'urgence décentralisé dénommé DEMP (Decentralized Emergency Management Protocol) et à l'implémenter de manière expérimentale au moyen de l'application prototype de sécurité personnelle OASIS (Open Alert and Safety Information System).

Les objectifs spécifiques de recherche sont les suivants :

- Élaborer une première version du DEMP, un protocole de communication dédié à la gestion des situations d'urgence décentralisé.
- Implémenter l'architecture du protocole dans un prototype d'application (OASIS) à des fins de preuve de concept.
- Simuler les concepts fondamentaux du DEMP grâce à l'application OASIS et évaluer les résultats.

Les résultats attendus de ce mémoire ont pour objectif de proposer une approche innovante, décentralisée et digitalisée de la gestion des situations d'urgence, dont l'ambition ultime est d'ouvrir la voie à un « réseau social de la sécurité personnelle ».

2. Gestion des situations d’urgence

2.1 Cycle en 5 phases

La gestion des situations d’urgence, d’un point de vue systémique, est souvent décrite à travers un cycle de 5 phases interconnecté, chacune jouant un rôle avant, pendant et après une crise. Ce cycle présente une approche stratégique pour faire face aux situations urgences, en reconnaissant que les activités couvrent plusieurs phases et que les frontières entre elles sont rarement distinctes (Farazmand 2001; Sabri et al. 2024).

2.1.1 Prévention

La prévention concerne la réduction des risques avant qu'ils ne puissent déboucher sur une situation d’urgence. Bien que tous les risques ne puissent être évités ou éliminés, des mesures préventives telles que la planification stratégique et l’adoption de normes peuvent contribuer à réduire les conséquences humaines et matérielles. Les activités de cette phase incluent notamment :

- **Évaluation des risques** : Identification et évaluation des dangers et menaces potentiels.
- **Planification** : Élaboration de stratégies pour minimiser les risques identifiés.
- **Sensibilisation** : Éducation des communautés sur les pratiques de sécurité et de prévention.

2.1.2 Préparation

La phase de préparation vise à s'assurer que les personnes et organisations sont prêtes à répondre à une situation d’urgence de manière efficace et efficiente. Cela inclut essentiellement la formation et l’allocation suffisante de ressources pour répondre à un danger particulier. Les activités clés incluent de cette phase :

- **Formation** : Programmes de formation réguliers pour le personnel et les intervenants.
- **Simulations** : Exercices pour tester les plans, identifier les lacunes et entraîner les intervenants.
- **Ressources** : Allocation de ressources et d'équipements pour les situations d'urgence.

2.1.3 Réponse

La réponse est l'action immédiate prise pour préserver des vies, limiter les dommages matériels et réduire les pertes économiques. Cela implique une coordination optimale entre de différents acteurs, notamment les services d’urgence, les partenaires privés, les institutions locales et les citoyens. Les activités clés incluent :

- **Prise de décision** : Évaluation rapide de la situation et conduite efficace des opérations sur le terrain.
- **Communication** : Mise en œuvre d'un protocole de communication ouvert et commun à tous les intervenants.
- **Partage d l'information** : Assurer le partage d'informations pertinentes entre tous les intervenants.

2.1.4 Rétablissement

La phase de rétablissement se concentre sur la capacité de résilience des personnes, communautés et organisations après une situation d'urgence. Une fois que la situation d'urgence est terminée, les efforts se concentrent essentiellement sur le rétablissement des victimes, le debriefing avec les intervenants et la compensation des dommages matériels et économiques. Les activités clés incluent :

- **Audit** : Évaluation des conséquences humaines, matérielles et économiques.
- **Soutien** : Assistance psychologique, financière et logistique pour les efforts de rétablissement.
- **Reconstruction** : Initiatives communautaires et indemnisations pour un rétablissement durable.

2.1.5 Atténuation

L'atténuation vise à réduire l'impact des catastrophes et des urgences futures. Les efforts d'atténuation tirent parti des retours d'expérience, des constats et bilans inhérent à la situation d'urgence. Les activités clés incluent :

- **Réglementation** : Audit et mises à jour des réglementations impliquées dans la situation d'urgence.
- **Planification** : Développement de politiques, procédure et formations pour minimiser les risques.
- **Amélioration continue** : Propositions et initiatives visant à évaluer et améliorer l'ensemble des moyens et processus mis en œuvre pour résoudre la situation d'urgence.

2.2 Paradigmes

Dans le cadre de la gestion des situations d'urgence, deux paradigmes distincts se démarquent et orientent la recherche académique (Liu 2023) : la centralisation et la décentralisation. En termes de gestion des situations d'urgence, chacune de ces approches possède ses avantages et inconvénients en matière prise de décision, de communication et partage de l'information.

2.2.1 Approche centralisée

La centralisation repose essentiellement sur une autorité centrale chargée de prendre des décisions, mobiliser, coordonner et contrôler l'ensemble des ressources nécessaires à la résolution d'une situation d'urgence. Il s'agit de l'approche traditionnellement utilisée par les services d'urgences (Liu 2023; Kapucu, Garayev 2011).

Les avantages :

- Niveau d'expertise des intervenants constant.
- Évaluation et allocation des ressources rationnelle.
- Partage du retour d'expérience entre organisations à des fins d'amélioration continue.

Les inconvénients :

- La gouvernance et la conduite des opérations peuvent être freinées par des contraintes institutionnelles, politiques et économiques.
- Point de défaillance unique : en cas de dysfonctionnement ou indisponibilité de l'autorité centrale, l'ensemble du processus de gestion est affecté (Liu 2023).
- Manque de flexibilité et d'adaptation aux spécificités locales inhérentes à une situation d'urgence, telle que l'intégration des secouristes locaux ou des volontaires (Skar, Sydnes, Sydnes 2016).

Les faiblesses de cette approche ont été mises en évidence sur le plan organisationnel lors de différentes situations d'urgence de grande ampleur telles que la gestion de la pandémie de COVID-19 en Suisse. En effet, dans un rapport publié par la Confédération en décembre 2020, la chancellerie fédérale souligne que la collaboration avec les cantons a été problématique en termes de délimitation des tâches, des compétences et des responsabilités durant la phase de situation extraordinaire de la pandémie (les 6 premiers mois). Il est également fait mention d'un manque de consultation des cantons avant certaines prises de décision, de problèmes d'interopérabilité dans la transmission d'informations et d'une communication interne sujette à des retards et imprécisions (ChF). En France, durant la même période, une étude a mis en exergue les tensions et problèmes de coordination ayant émergé entre l'État, hypercentralisé, et les collectivités locales, avec une emphase sur les bénéfices obtenus par ces dernières lorsqu'elles ont mise en œuvre un mode de gouvernance orienté vers la décentralisation (Du Boys, Bertolucci 2021).

La littérature (Farazmand 2001) suggère que l'approche centralisée pose essentiellement un problème au début de la phase de réponse à la situation d'urgence. Notamment lorsque l'événement est rare ou extraordinaire par son ampleur et lorsque les gouvernements et intervenants locaux, qui souvent possèdent une meilleure

connaissance du terrain et des communautés, ne sont pas sollicités immédiatement et activement par l'autorité centrale.

2.2.2 Approche décentralisée

L'approche décentralisée se caractérise par une délégation des responsabilités, du processus de décision et de la coordination à différents niveaux et intervenants, notamment auprès des gouvernements locaux, des communautés et volontaires, avec pour effet une réponse plus rapide, s'appuyant sur une plus grande flexibilité structurelle (Liu 2023; Kapucu, Garayev 2011).

Les avantages :

- Plus d'autonomie et auto-organisation des institutions locales et volontaires.
- La coordination, la communication et l'échange d'informations s'effectuent avec l'implication renforcée des institutions locales, des volontaires et, dans certains cas, avec l'appuis des réseaux sociaux (Panagiotopoulos et al. 2016).
- Offre une plus grande flexibilité et adaptation au contexte local et permet réponse immédiate sur le terrain (Liu 2023).
- Les volontaires jouent un rôle prépondérant dans la gestion de crise en apportant une réponse immédiate à la situation d'urgence.

Les inconvénients :

- La délégation de l'autorité et des responsabilités est informelle.
- Le partage d'informations entre l'ensemble des intervenants biaisé, excessif ou impossible.
- Possibles incompatibilités dans les formats d'échange de données.
- Différences culturelles et linguistiques.
- Niveau d'expertise des intervenants variable et imprévisible.
- Allocation de ressources disproportionné (Liu 2023).
- Hétérogénéité des moyens de communication.

2.2.3 Approche hybride

Selon (Liu 2023), une approche innovante pourrait consister à exploiter les avantages de chacune de ces deux approches. Le cas échéant, la centralisation garantirait un processus de décision global et une allocation optimale des ressources, tandis que la décentralisation tirerait avantage du contexte local, de la communauté et des volontaires avec, à la clé, une réponse plus rapide. Enfin, il est souligné que l'usage des nouvelles technologies, notamment des algorithmes d'intelligence artificielle, du big data, des objets connectés ou encore de la technologie Blockchain (El-Sayed, Abdelaziz, Abdel-

Azeem 2023), permettrait d'agir plus efficacement lors de situations d'urgence en fournissant des informations consistantes et un degré de transparence élevé pour le public.

2.3 Prise de décision

La prise de décision est un pilier de la gestion des situations d'urgence. (Kapucu, Garayev 2011) souligne qu'il s'agit d'un processus fondamentalement influencé par :

- Par la complexité et l'ampleur de la situation d'urgence.
- L'implication de plusieurs organisations et catégories d'intervenants dans la conduite des opérations.
- Le climat d'incertitude créé par une atmosphère chaotique.
- La nécessité de prendre des décisions immédiates et à hauts risques.

Lors catastrophes naturelles et humaines de grande ampleur ont démontré les limites de la centralisation en termes de gestion (Farazmand 2001), cela au profit de la décentralisation, davantage axée sur la collaboration, la flexibilité structurelle et opérationnelle. Afin d'améliorer la prise de décision lors des situations d'urgence, des nouveaux outils et modèles de décision collaboratifs ont été conceptualisés. Ces techniques visent à améliorer les compétences organisationnelles et individuelles, notamment dans le cadre de la gestion de crise (Kapucu, Garayev 2011).

Toujours selon (Kapucu, Garayev 2011) « *la collaboration intervient lorsque des acteurs de différentes organisations produisent conjointement quelque chose en mettant en commun les ressources et processus décisionnels dans le but de bénéficier conjointement du résultat final* », l'étude souligne par ailleurs que le résultat et l'efficacité constituent les aspects les plus importants d'une collaboration.

2.3.1 Modèles

Un modèle analytique-heuristique décrit un extrême où la prise de décision repose uniquement sur l'analyse des données et les informations techniques tandis que l'autre extrême s'appuie exclusivement sur le jugement heuristique, c'est à dire l'expérience et les circonstances opérationnelles. Un troisième modèle concerne le nombre de décideurs impliqués, allant d'un seul individu ou organisation à un maximum de décideurs individuels ou organisations dans un contexte spécifique (Kapucu, Garayev 2011).

La littérature s’accorde en pratique sur le fait que les situations d'urgence sont trop complexes et sujettes au changement pour être gérées exclusivement par l’analyse de données (Kapucu, Garayev 2011).

Pour une prise de décision optimale en situation d'urgence, il est nécessaire de combiner à la fois des outils analytiques et heuristiques, de favoriser la collaboration entre différents intervenants et de gérer les facteurs d'incertitude de manière appropriée, cela passe notamment par la formation et les systèmes d’aide à la décision (Kapucu, Garayev 2011).

2.4 Interopérabilité

L'interopérabilité se réfère à la capacité des organisations et individus à s'adapter à des environnements, cultures, moyens de communication et de partage de l’information hétérogènes. Cette capacité est essentielle dans le contexte de la gestion des situations d’urgence, et plus particulièrement dans un environnement décentralisé s’appuyant sur un modèle de décision collaboratif.

La principale difficulté liée à l'interopérabilité réside dans la cohésion et la coordination de l’ensemble des intervenants, chacun apportant ses propres effectifs, méthodes et processus. Viennent s’ajouter à cela les volontaires, qui constituent souvent une ressource sous-utilisée en raison des difficultés d'intégration dans des systèmes de réponse de réponse centralisés. Comme le souligne (Skar, Sydnes, Sydnes 2016), l’implication de volontaires est d’ailleurs souvent perçue négativement par les professionnels, qui peinent à les gérer en raison du niveau d’expertise variant et imprédictible, et combien plus dans un environnement inter-organisationnel.

Ces différences peuvent perturber le processus de décision, entraîner des délais et des erreurs d’interprétation. En outre, des problèmes peuvent survenir sur le plan humain, lorsque des personnes n’ont pas travaillé ensemble auparavant ou si des différences culturelles notables empêchent une communication fluide, telles que la langue.

Pour améliorer l'interopérabilité, il est nécessaire de développer un protocole commun et des outils de communication compatibles entre toutes les organisations et individus impliqués dans la gestion de la situation d’urgence.

L'interopérabilité exige également un niveau élevé de confiance et de coopération entre les parties. Les organisations doivent être prêtes à partager des informations de manière transparente et à collaborer étroitement pour atteindre des objectifs communs. Cela

implique de surmonter les barrières culturelles et organisationnelles et de s'engager à travailler ensemble, et de manière improvisée lorsque les situations l'exigent.

Enfin, pour renforcer l'interopérabilité, des formations et des exercices de simulation sont à préconiser afin de préparer les personnels et volontaires à travailler dans des environnements organisationnels ad hoc et complexes. Ces formations devraient se concentrer sur le développement de compétences en communication et en coordination, ainsi que sur la familiarisation avec des outils utilisés ou utilisables par tous les intervenants (Kapucu, Garayev 2011).

L'interopérabilité n'est pas seulement une question de culture organisationnelle et de relations humaines, elle est en pratique intrinsèquement liée aux technologies de l'information et de la communication.

2.5 Communication

La communication joue un rôle fondamental dans la décentralisation et la prise de décision collaborative lors des situations d'urgence. Elle assure le transfert, la réception, l'intégration et l'exploitation des connaissances entre les intervenants.

Dans le contexte de la gestion des situations d'urgence, une communication efficace repose sur plusieurs critères :

- **L'intégrité** : des informations provenant de sources hétérogènes peuvent être partielles, faussées ou erronées, conduisant à de mauvaises décisions sur le terrain. **La qualité doit être privilégie sur la quantité**.
- **La disponibilité** : l'absence ou la rétention d'information peuvent entraîner des délais et conflits entre intervenants.
- **La confidentialité** : le respect de la vie privée et la protection des données est essentielle à la conduite des opérations.

L'engagement des organisations envers la communication est également un facteur déterminant. Cet engagement peut varier de la compétition, où il n'y a pas de confiance dans les informations échangées, à la collaboration, où il y a un accord mutuel pour travailler ensemble sur les mêmes tâches (Dunn, Lewandowsky, Kirsner 2002). Pour que la prise de décision collaborative soit optimale, les organisations et intervenants doivent être en mesure de viser le plus haut niveau de cette échelle, c'est-à-dire la collaboration, ce qui nécessite une évaluation précise des capacités et des objectifs de chaque organisation impliquée, en tenant compte de l'intégration des volontaires.

2.6 Partage de l’information

Le partage de l'information est le pilier de la gestion des situations d'urgence. Une communication efficace et une distribution rapide et précise des informations peuvent considérablement améliorer la prise de décision et la conduite des opérations.

La capacité à partager des informations entre les intervenants est essentielle car les premières minutes suivant le début d’une situation d’urgence sont souvent les plus critiques, en particulier pour préserver des vies. Un partage immédiat et en temps-réel permet en effet aux témoins (premier répondants) et secouristes de recevoir des renseignements critiques sur type le d’urgence, l’environnement et la localisation des personnes en danger.

La qualité des décisions prises pendant une crise dépend directement de la qualité des informations disponibles (Kapucu, Garayev 2011). Des informations précises et à jour permettent en effet aux intervenants de mieux appréhender l'étendue de la situation et de prendre de meilleures décisions, plus rapidement.

Enfin, le partage d'informations améliore la transparence des opérations et permet une meilleure supervision des opérations et retour d’expérience de la part des intervenants.

2.7 Systèmes d’information

Dans la littérature, trois principales approches ont été identifiées pour interconnecter les systèmes d’information d’urgence : les liens décentralisés un-à-un, les plateformes d'information centralisées et les plateformes d'échange d'informations centralisées.

2.7.1 Approche décentralisée un-à-un

Dans cette approche, le partage de l’information s’effectue directement entre les intervenants en exploitant une variété de technologies différentes, allant du téléphone au courriel (Holzhüter, Meissen 2020) en passant par la messagerie instantanée.

2.7.2 Plateformes d’information centralisées

Pour pallier les limitations d’une architecture “un à un”, des chercheurs ont développé des plateformes d’information centralisées. Il s’agit bases de connaissances rassemblant des informations provenant de différentes sources (Holzhüter, Meissen 2020).

2.7.3 Plateformes d’échange d’informations centralisées

Les plateformes d'échange d'informations centralisées ont pour objectif d’apporter une dimension dynamique aux bases de connaissance. Ces plateformes agissent comme

des hubs d'échange, où les données sont directement transmises entre les parties prenantes via un médiateur, sans être stockées sur la plateforme elle-même (Holzhüter, Meissen 2020).

2.7.4 Plateforme d'échange d'information décentralisée

Une architecture décentralisée permettant d'interconnecter les systèmes d'information peut contribuer à surmonter les limitations de l'ensemble de ces systèmes traditionnels en offrant une plus grande rapidité de réponse et de meilleures garanties en termes de sécurité.

Elle réunit notamment les avantages suivants :

- **Disponibilité accrue** : Une architecture décentralisée ne dépend pas d'un point de défaillance unique. Si une partie du réseau est compromise ou indisponible, les autres parties peuvent continuer à fonctionner, assurant ainsi une continuité des opérations.
- **Flexibilité et adaptabilité** : Les systèmes décentralisés peuvent facilement s'adapter à des situations changeantes. De nouvelles entités peuvent être intégrées au réseau sans perturber l'ensemble du système, permettant une montée en charge et réponse adaptée à la gestion des situations d'urgence.
- **Rapidité de réponse** : En éliminant la nécessité de passer par une autorité centrale pour la validation ou la distribution des informations, les systèmes décentralisés permettent un partage d'informations plus rapide et réactif.

2.7.5 Le rôle du DEMP

La conception du DEMP a pour objectif de tirer avantage non seulement d'une architecture décentralisée pour le partage de l'information mais aussi de moyens de communications et de collaboration modernes, **pour une gestion agile des situations d'urgence**.

2.7.5.1 Sécurité

La sécurité est la pierre angulaire du DEMP. L'architecture décentralisée renforce en effet la confidentialité, l'intégrité et la disponibilité de l'information en s'appuyant sur une infrastructure intégrant des mesures de chiffrage robustes et des mécanismes de résistance aux pannes éprouvés.

2.7.5.2 Coordination

En l'absence d'une autorité centrale, le DEMP met en œuvre des mécanismes de gouvernance décentralisés s'appuyant sur des décisions collaboratives fondées sur le consensus, assurant ainsi une coordination optimale entre les différents intervenants en toute circonstance.

2.7.5.3 Transparence

En tant que protocole ouvert, le DEMP encourage la transparence. Les mécanismes et recommandations en matière de communication, de gestion des données, et de coordination sont conçus pour être audités par des tiers indépendants, assurant ainsi un contrôle complet des processus. Cette transparence est essentielle pour instaurer la confiance parmi les parties prenantes et le public, en particulier dans le contexte des situations d'urgence où la précision et la fiabilité sont vitales.

3. Protocole DEMP

3.1 Vue d’ensemble

Le Decentralized Emergency Management Protocol (DEMP) est une première version de protocole de gestion d’urgence décentralisé ayant pour objectif d’assurer la connectivité et l’interopérabilité des systèmes d’information de sûreté en temps de crise.

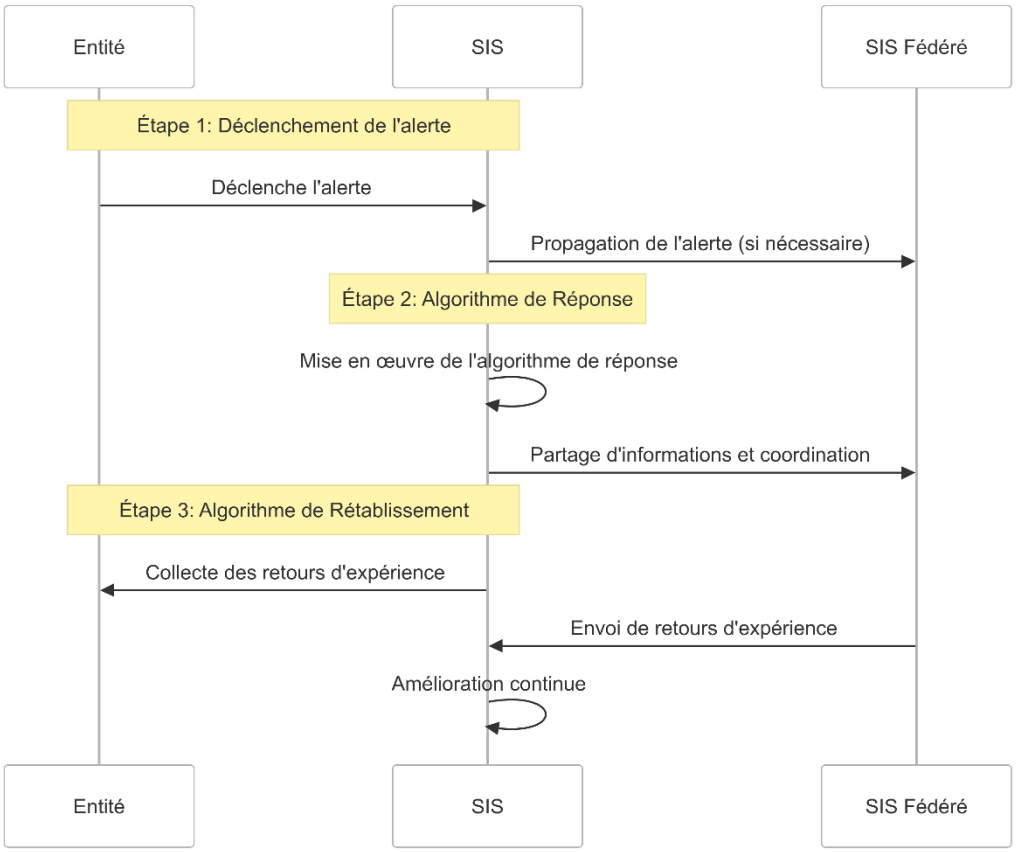
Le DEMP vise à surmonter les limitations des architectures centralisés traditionnelles, qui peuvent être vulnérables et sujettes à des restrictions organisationnelle et techniques.

Le DEMP est structuré autour d'une architecture décentralisée fondamentalement composée d’un Système d’Information de Sûreté (SIS), de zones de sûreté et d’entités.

Le DEMP est un standard ouvert, ce qui signifie que ses recommandations conceptuelles et techniques ont vocation à être librement accessibles à tout individu, ou organisation souhaitant les implémenter ou les améliorer. Cette ouverture vise à encourager l'adoption généralisée du DEMP, à faciliter l'interopérabilité et à promouvoir l'innovation dans le domaine de la gestion des urgences digitalisées.

3.2 Processus

Figure 1 : Processus DEMP



Le processus DEMP constitue un ensemble d'activités tirant partie du Cycle en 5 phases de gestion des situations d'urgence. Il s'appuie respectivement sur la phase de Réponse et de Rétablissement et peut être décrit en 3 étapes distinctes : le déclenchement d'une alerte, l'algorithme de réponse et l'algorithme de rétablissement.

3.2.1 Déclenchement de l'alerte

La première étape est le déclenchement de l'alerte. Ele peut être déclenchée par le Système d'Information de Sûreté (SIS), respectivement, son administrateur, par une entité présente dans l'un des zones du SIS ou par l'un des SIS fédérés.

3.2.2 Algorithme de Réponse

La seconde étape est la mise en œuvre de l'algorithme de réponse. L'algorithme de réponse est un ensemble d'activités spécifiques à un type de situation d'urgence qui doivent être mises en œuvre séquentiellement ou simultanément par le Système d'Information de Sûreté en fonction de l'évolution de la situation d'urgence.

3.2.3 Algorithme de Rétablissement

La troisième étape est la mise en œuvre de l'algorithme de rétablissement. Cet algorithme vise à collecter un retour d'expérience de la part des personnes et organisations impliquées dans la gestion de la situation d'urgence, il a vocation à permette l'amélioration continue.

3.3 Fondamentaux

3.3.1 Client

Un Client est un appareil, dispositif ou composant informatique doté d'une interface réseau permettant la réception et le transfert de données sur un réseau IP (*Internet Protocol* 1981).

3.3.2 Serveur

Un Serveur est un système informatique matériel ou logiciel fournissant des services en réponse à des requêtes en provenance d'un Client via un réseau IP. Il est identifié par une adresse IP et (obligatoirement dans le cas du DEMP) un nom de domaine DNS (*Domain names - implementation and specification* 1987).

3.3.3 Réseau

Un Réseau informatique est constitué d'un ensemble d'ordinateurs, de serveurs, de dispositifs et d'autres équipements connectés entre eux afin de partager des ressources, échanger des données, et communiquer. Les réseaux peuvent être constitués de plusieurs Clients (appelés aussi hôtes) qui se connectent soit via des serveurs (modèle client-serveur) soit directement entre eux (modèle P2P).

3.3.4 Fédération

Une fédération désigne l'interconnexion d'un ensemble de serveurs, éventuellement situé dans des réseaux IP distincts, configurés pour communiquer et interagir entre eux de manière sécurisée. Cette communication inter-serveur permet de partager des informations et de coordonner des actions de manière concertée et transparente.

3.3.5 Système d'Information de Sûreté

Un Système d'Information de Sûreté (SIS) assure la collecte, le traitement et l'échange d'informations entre les entités connectées et les autres SIS. Il est composé de zones de sûreté, d'entités et appareils associés à celles-ci.

Un Système d'Information de Sûreté possède un propriétaire, un responsable administratif et un responsable technique. Les rôles peuvent être occupés par une seule personne ou par une organisation.

3.3.6 Entité

Une entité représente un ou plusieurs appareils informatiques au sein d'un système d'information de sûreté (SIS). Une entité peut représenter une personne, une organisation, un logiciel ou du matériel. Cette qualification est fournie sous forme de métadonnée et peut être exploitée par le SIS dans la gestion d'une situation d'urgence.

Tableau 1 : Types d'entités DEMP

Type	**Description**
ch.demp.entity.type.individual	Individu
ch.demp.entity.type.organization	Organisation
ch.demp.entity.type.organization	Logiciel
ch.demp.entity.type.hardware	Matériel

3.3.7 Appareil

Une entité peut être constituée d'un ou plusieurs appareils informatiques (Device) pouvant se connecter simultanément à un SIS depuis différent endroits. Un appareil peut être de type passif ou actif. Un appareil passif fournit des informations en lecture seule au système d'information de sûreté tandis qu'un appareil actif peut interagir avec celui-ci.

Tableau 2 : Types d'appareils DEMP

Type	**Description**
ch.demp.device.type.active	Ppeut interagir avec le SIS et les autres entités.
ch.demp.device.type.passive	Transmet des informations uniquement.

Un appareil, indépendamment de son type, devrait transmettre au minimum les métadonnées suivantes lors de chacune de ses interactions avec un SIS :

- Son identifiant
- Le type d'appareil (passif ou actif)
- L'entité à laquelle il appartient.
- Lorsqu'un appareil se situe dans une zone de sûreté physique, son emplacement doit être exprimé sous forme de coordonnées cartésiennes.
- La catégorie d'appareil (ordinateur de bureau, téléphone mobile, objet connecté, etc.)

3.3.8 Annuaire

Une Système d'Information de Sûreté doit indexer les zones de sûreté publiques et proposer un annuaire consultable librement par les entités désireuses de se renseigner.

3.3.9 Zone de sûreté

Une zone de sûreté (abrégée zone) représente un périmètre physique ou virtuel. Une zone peut être permanente ou temporaire. Elle peut être créée à l'avance ou de manière « ad hoc » pour une durée ou un événement spécifique.

3.3.9.1 Zone physique

Une zone de sûreté physique est délimitée par un périmètre et son emplacement par des coordonnées géospatiales.

3.3.9.2 Zone virtuelle

Une zone de sûreté virtuelle possède les mêmes attributs qu'une zone physique à l'exception qu'elle n'est pas définie par des coordonnées géospatiales.

Tableau 3 : Types de zone de sûreté DEMP

Type	**Description**
ch.demp.zone.type.actual	Zone physique
ch.demp.zone.type.virtual	Zone virtuelle (logique)

3.3.9.3 Accès

Une entité peut rejoindre une zone librement ou exclusivement sur invitation. Lorsque l'entité peut rejoindre librement une zone, cette zone est dite en accès public, lorsque que l'entité doit être invitée au préalable, cette zone est dite en accès privé.

Tableau 4 : Accès aux zones de sûreté DEMP

Accès	**Description**
ch.demp.zone.acces.public	Une entité peut rejoindre librement la zone de sûreté.

ch.demp.zone.access.private	N’apparaît pas publiquement.

3.3.9.4 Visibilité

Une zone de sûreté en visibilité publique est indexée dans l’annuaire des zones du Système d’Information de Sûreté, ainsi que dans les annuaires des SIS fédérés.

Une zone de sureté en visibilité privée n’est pas indexée dans les annuaires, son existence doit être annoncé par un responsable du SIS auprès des groupes et personnes concernées.

Tableau 5 : Visibilité des zones de sûreté DEMP

Visibilité	**Description**
ch.demp.zone.visibility.public	Apparaît par défaut dans les annuaires des Système d’Information de Sûreté
ch.demp.zone.visibility.private	N’apparaît pas publiquement.

3.3.9.5 Métadonnées géospatiales

Une zone de sûreté physique représente une aire et un périmétrie réels définis par des coordonnées géospatiales statiques ou dynamiques. Ces métadonnées sont exploitées en cas d’alerte déclenchée depuis ladite zone, et peuvent être exploitées par les SIS pour fournir une aide à la décision lors d’une situation d’urgence.

Une zone de sûreté virtuelle constitue un périmètre de sûreté logique ne faisant pas référence à un emplacement physique réel. Toutes les entités appartement à ce type de zones sont susceptibles de recevoir des alertes, indépendamment du lieu géographique dans laquelle elles sont situées.

Tableau 6 : Métadonnées géospatiales des zones de sûreté DEMP

Métadonnée	**Description**
ch.demp.zone.metadata.latitude	Latitude (en degrés)
ch.demp.zone.metadata.longitude	Longitude (en degrés)
ch.demp.zone.metadata.length	Longueur (en mètres)

ch.demp.zone.metadata.width	Largeur (en mètres)
ch.demp.zone.metadata.perimeter	Périmètre (en mètres)
ch.demp.zone.metadata.area	Aire (en mètres carrés)

3.3.10 Alerte

Une alerte se compose fondamentalement d'un identifiant, d'un type, d'une source, d'une visibilité et d'un niveau de sévérité.

3.3.10.1 Niveaux de sévérité

La classification des alertes est essentielle pour la gestion des situations dans leur ensemble car elles permettent d'évaluer de manière précise la gravité de la situation et d'adapter la réponse du Système d'Information de Sûreté (SIS) en conséquence. Chaque niveau de sévérité est associé à des critères de gravité spécifiques. Le niveau de sévérité d'une alerte peut être escaladé ou désescaladé en fonction de l'évolution de la situation.

Tableau 7 : Niveaux de sévérité des alertes DEMP

Niveau de sévérité	**Description**	**Exemples**
Niveau 1	Message d'information	Sans gravité, destiné à diffuser des messages d'information exclusivement.
Niveau 2	Avertissement	La vigilance des entités est requise. Le message d'alerte doit être acquitté par l'entité.
Niveau 3	Alerte modérée	Une action est requise de la part des entités afin de répondre à la situation d'urgence.
Niveau 4	Alerte grave	Une urgence avec un risque élevé de préjudice nécessitant une réponse immédiate.
Niveau 5	Alerte critique	Une urgence majeure avec danger de mort imminente ou de dommages potentiels de grande ampleur.

3.3.10.2 Escalade et désescalade du niveau d'alerte

L'escalade ou la désescalade d'une alerte se produit lorsque la situation évolue en devenant plus ou moins grave qu'initialement estimée. Sont habilités à changer le niveau d'une alerte : les entités bénéficiant du statut Vérifié+ et les SIS appartenant aux services d'urgences fédérés. En l'absence de ceux-ci, l'alerte peut être mise à jour par consensus des entités présentes.

3.3.10.3 Statut d'alerte

Chaque alerte suit un cycle caractérisé par plusieurs statuts distincts permettant de suivre l'évolution de la situation d'urgence et d'adapter l'algorithme de réponse ne conséquence.

Tableau 8 : Statuts d'alerte DEMP

Statut	**Description**
Alerte déclenchée	Statut initial lorsqu'une alerte est déclenchée par le Système d'Information de Sûreté ou une entité.
Alerte en cours	Indique que l'alerte a été confirmée et que la phase de réponse est mise en œuvre pour gérer la situation d'urgence.
Alerte escaladée	La situation s'est aggravée et nécessite l'adaptation de la réponse en conséquence.
Alerte désescaladée	La situation s'est améliorée et nécessite l'adaptation de l'algorithme de réponse.
Alerte annulée	Indique que l'alerte est annulée à la suite d'un déclenchement accidentel ou malveillant.
Alerte résolue	Indique que la phase de réponse à la situation d'urgence est terminée.

3.3.10.4 Consensus

Un consensus peut être requis pour mettre à jour le niveau de sévérité d'une alerte ou son statut si les conditions sur le terrain sont changeantes et qu'il n'y a pas d'autorité légitime en activé dans la zone de sûreté.

Plus concrètement, si une partie des entités considère que la situation s'aggrave, un consensus peut être atteint par vote pour escalader le niveau de sévérité. Inversement, si les entités perçoivent une amélioration générale, elles peuvent décider collectivement de désescalader l'alerte. Dans le même ordre d'idées, si le statut d'une alerte est

contesté, un consensus peut être atteint pour annuler l'alerte ou la considérer comme résolue.

3.3.10.5 Autorité

Seules les entités disposant du statut Vérifié+ ainsi que les Systèmes d'Information de Sûreté fédérés des services d'urgence sont habilités à changer le niveau d'une alerte ou sa sévérité sans nécessiter de consensus.

3.3.11 Alerte ouverte

L'Alerte ouverte est un concept dont l'objectif est de propager des messages d'alerte en cascade sur un nombre déterminé ou indéterminé de zones de sûreté et Systèmes d'information de Sûreté (SIS), selon sa visibilité. Un diagramme de séquence est disponible en Annexe 1.

La visibilité d'une alerte est dite « de zone » lorsqu'elle doit se propager uniquement dans la zone de sûreté dans laquelle elle a été déclenchée. Une alerte est dite « système » lorsqu'elle peut être propagée à toutes les zones du SIS. Une alerte est dite « fédérée » lorsqu'elle peut être propagée à des zones situées sur un ou plusieurs SIS fédérés. Enfin, une alerte est dite « ouverte » lorsqu'elle peut être propagée à l'ensemble des zones du SIS, des SIS fédérés et éventuellement à tous les autres SIS auxquels les SIS fédérés sont liés.

3.3.11.1 Alerte de zone

L'alerte de zone sera propagée uniquement dans la zone source dans laquelle l'alerte a été déclenchée.

3.3.11.2 Alerte système

L'alerte système sera propagée à la zone source et à toutes les zones du système d'information de sûreté.

3.3.11.3 Alerte fédérée

L'alerte fédérée sera propagée à la zone source ainsi qu'aux Systèmes d'information de Sûreté fédérés.

3.3.11.4 Alerte ouverte

L'alerte ouverte sera propagée à la zone source, à toutes les zones du Système d'information de Sûreté (SIS), aux SIS fédérés et au-delà.

Tableau 9 : Visibilité d'une alerte ouverte DEMP

Visibilité de l'alerte	**Description**
ch.demp.alert.visibility.zone	Alerte limitée à la zone de sûreté source.
ch.demp.alert.visibility.system	Alerte propagée à l'ensemble des zones de sûreté du SIS originel.

ch.demp.alert.visibility.federated	Alerte propagée à la zone de de sûreté originelle et aux SIS fédérés.
ch.demp.alert.visibility.open	Alerte propagée à toutes les zones du SIS originel, aux SIS fédérés et potentiellement au-delà.

3.3.12 **Agent d'Alerte**

L'Agent d'Alerte est agent autonome chargé de gérer la réception, le déclenchement et la gestion des alertes au sein d'un Système d'Information de Sûreté (SIS). Il joue le rôle d'orchestrateur en observant les événements intervenant dans les zones de sûreté.

- Traiter le déclenchement des alertes par les entités connectées au SIS courant.
- Évaluer le type et la sévérité de l'alerte
- Diffuser l'alerte à la (ou les) zones du SIS.
- Gérer l'algorithme de Réponse
- Gérer l'algorithme de Rétablissement

3.3.13 Agent de Test

L'Agent de Test est un agent autonome dont la tâche consiste à effectuer des diagnostiques de fonctionnement à la demande.

• Tester à la demande la connectivité d'une entité avec le SIS.

• Tester l'Agent d'Alerte en déclenchant des alertes de test.

3.3.14 Agent de Surveillance

L'Agent de Surveillance (MonitoringAgent) est un agent autonome chargé de vérifier continuellement le fonctionnement des autres agents autonomes et de signaler toute anomalie technique au sein du Système d'Information de Sûreté.

Les tâches de l'Agent de Surveillance consistent à :

- Tester la présence et le bon fonctionnement des Agents en continue
- Signaler les anomalies au responsable technique du Système d'information de Sûreté
- Effectuer des tâches de maintenance.

3.3.15 Agent Générique

L'Agent Générique (GenericAgent) est un agent autonome permettant d'émuler le comportement d'une entité ou un appareil en permettant des interactions et l'envoi de données fictives au Système d'Information de Sûreté (SIS).

Les tâches de l'Agent générique consistent à :

- Émuler le comportement d'une entité en rejoignant des zones de sûreté.
- Émuler le comportement d'un appareil, par exemple en transmettant des données géospatiales durant une alerte.
- Interagir avec les autres agents autonomes du SIS à des fins de simulation.

3.4 Partage de l'information

Le partage de données la pierre angulaire du DEMP, assurant une communication sécurisée et en instantanée entre les différentes entités, zones et systèmes d'information de sûreté (SIS) impliqués dans la gestion d'une situation d'urgence.

3.4.1 Espaces de nom

Les espaces de nom ont pour objectif d'organiser les données en ensemble structurés et uniques en termes de responsabilités et rôles au sein du DEMP. Ces espaces de nom servent essentiellement à améliorer la compréhension, la lisibilité et l'implémentation du protocole. Les identifiants d'espace de nom s'appuient sur la notation utilisée pour nommage des paquetages Java (*Naming a Package (Java™)*).

Tableau 10 : Espaces de nom DEMP

Identifiant	**Description**
ch.demp.alert	Données concernant les alertes
ch.demp.entity	Données concernant les entités
ch.demp.device	Données concernant les appareils
ch.demp.zone	Données concernant les Zones de sûreté
ch.demp.sis	Données concernant les Systèmes d'Information de Sûreté

3.4.2 Format des données

Le format des données échangées dans le cadre du DEMP a vocation à assurer l'interopérabilité et la cohérence des informations à travers différents systèmes et plateformes de traitement de données.

3.4.2.1 JSON

JSON (JavaScript Object Notation) est un format de texte dédié à l'échange de données (*JSON*). Il est léger, lisible, et facilement exploitable grâce à une syntaxe simple composée de paires de clé-valeur. La plupart des langages de programmation

fournissent des librairies natives assurant une prise en charge robuste en termes de lecture, écriture et stockage.

3.4.2.2 XML

XML (Extensible Markup Language) est un format de texte et langage de balisage (markup language) dédié à l'échange de données. Il a été conçu à l'origine pour être simple et flexible en permettant la structuration, le traitement et la transformation de données et documents textuels au sein d'une variété d'environnement et d'applications.

Le tableau suivant établit un comparatif des formats JSON et XML.

Tableau 11 : Comparatif JSON / XML

Caractéristique	**JSON**	**XML**
Gestion	ECMA (*ECMA-404*) / IETF (Bray 2017)	W3C (*Extensible Markup Language (XML)*)
Type	Format de texte structuré.	Langage de balisage
Lisibilité	Léger, concis, facile à lire et à écrire.	Verbeux, peut devenir complexe, difficile à lire et à appréhender.
Comptabilité	Intégré nativement dans de nombreux langages de programmation.	Intégré nativement dans de nombreux langages de programmation.
Structure	Paires de clé-valeur délimitées par des guillemets, accolage et virgules, éventuellement imbriquées.	Hiérarchies de balises imbriquées composées d'espaces de nom, attributs et valeurs textuelles.
Performance	Conçu pour être économique en termes de stockage, de transmission et de traitement.	Verbeux et relativement lourd, l'optimisation de l'espace de stockage ou du temps de traitement ne sont pas des objectifs conceptuels clés.
Interopérabilité	Format d'échange préconisé pour les API RESTFul, pour le stockage de données ou l'élaboration de fichiers configuration.	Technologie mature et universelle pour l'interopérabilité entre les systèmes, applications et documents.

JSON est le format recommandé pour l'implémentation du DEMP car il comporte plusieurs avantages clés qui en font un format idéal pour l'échange de données au sein d'un Système d'Information de Sûreté. JSON est en effet un format léger permettant la transmission rapide et économique de données, essentielles dans les environnements où le débit de transfert, la puissance de calcul et l'économie de ressources peuvent être

critiques, en particulier dans un contexte de situation d'urgence associé à des contraintes de haute disponibilité.

3.4.3 Types de données

Le DEMP s'appuie sur un ensemble de types de données pour assurer la gestion optimale des situations d'urgence. Les données échangées peuvent varier en termes d'importance et de temporalité et sont organisées en plusieurs catégories pour répondre au mieux aux objectifs opérationnels du protocole.

Tableau 12 : Catégorie de types de données DEMP

Catégorie	**Description**
Données opérationnelles	Données ayant un impact direct sur la gestion d'une situation d'urgence.
Données de support	Données n'ayant pas d'incidence directe sur la gestion d'une situation d'urgence.

3.4.3.1 Données opérationnelles

Les données opérationnelles représentent les données d'exploitation du Système d'Information de Sûreté (SIS). Elles peuvent être statiques ou dynamiques et ont un impact direct sur la gestion de la situation d'urgence. Ces données sont déterminantes pour l'aide à la décision lors de la situation d'et peuvent avoir un impact direct sur la sécurité des personnes et des biens.

Le tableau suivant énumère les principaux types de données opérationnelles.

Tableau 13 : Types de données opérationnelles DEMP

Type de données	**Description**	**Exemples**
Données d'Alerte	Informations critiques lors du déclenchement d'une alerte et jusqu'à la fin de la gestion de la phase de réponse.	Type d'alerte, statut de l'alerte, sévérité, visibilité, zones de sûreté et SIS impliqués.
Données géospatiales	Informations permettant de localiser le lieu et l'emplacement des entités.	Latitude et longitude de la zone de sûreté, position de l'entité.
Données médicales	Informations inhérentes à l'état de santé d'une entité humaine.	Groupe sanguin, dossiers médicaux électroniques.

Données d'identification	Informations administratives permettant de garantir l'identité d'une entité.	Identifiants de documents officiels.
Données biométriques	Informations relatives aux caractéristiques physiques d'une personne.	Empreintes digitales, reconnaissance faciale, reconnaissance vocale.
Données administratives	Information administratives relatives à une personne.	Adresse postale, numéro de téléphone, contacts d'urgence.

3.4.3.2 Données de support

Les données de support sont collectées et exploitées de manière complémentaire par le SIS pour gérer une situation d'urgence. Elles ne sont pas décisives pour la prise de décision en temps réel et concernent uniquement des données statiques. Leur rôle est d'apporter un contexte supplémentaire et de favoriser l'amélioration continue.

Tableau 14 : Types de données de support DEMP

Catégorie	**Description**	**Exemples**
Données d'audit	Données collectées par le SIS durant la situation d'urgence.	Données relatives à l'état du système et des appareils.
Données historiques	Données n'ayant pas d'incidence directe sur la gestion d'une situation d'urgence.	Données d'audit collectées et traitées précédemment.
Données de feedback (retour d'expérience)	Données collectées durant la phase de rétablissement.	Retour d'expérience des utilisateurs.

3.4.4 Commandes

Le partage d'informations entre les Système d'Information de Sûreté (SIS) et entre les entités sont encadrées par un ensemble de commandes (signaux) standardisées. Ces commandes ont pour objectif de fournir une interface commune à tous les composants du système afin de garantir des interactions formelles, robustes et interopérables.

3.4.4.1 Système d'Information de Sûreté

Tableau 15 : Commandes de gestion des alertes DEMP

Commande	**Description**

ch.demp.sis.**poke**	Vérifie si une entité est active

3.4.4.2 Alerte

Tableau 16 : Commandes de gestion des alertes DEMP

Commande	**Description**
ch.demp.alert.**start**	Envoie d'une alerte
ch.demp.alert.**update**	Met à jour le statut d'une alerte
ch.demp.alert.**cancel**	Annule une alerte
ch.demp.alert.**stop**	Met fin à une alerte
ch.demp.alert.**forward**	Propagation d'une alerte
ch.demp.alert.**confirm**	Demande de confirmation

3.4.5 Événements

Les événements ont pour objectif de signaler un changement d'état au sein d'un Système d'Information de Sûreté (SIS) à un instant donné. Au même titre que les commandes, les événements visent à renforcer l'interopérabilité entre différentes implémentations de composants DEMP.

Tableau 17 : Événements génériques DEMP

Événement	**Description**
ch.demp.event.**alert**	Événement lié à une alerte.
ch.demp.event.**entity**	Événement lié à une entité.
ch.demp.event.**device**	Événement lié à un appareil
ch.demp.event.**zone**	Événement lié à une zone
ch.demp.event.**sis**	Événement lié à un SIS

3.5 Authentification

L'authentification permet de garantir que seules les entités autorisées et identifiées peuvent interagir avec un Système d'Information de Sûreté (SIS).

3.5.1 Connexion

La connexion à un Système d'information de Sûreté (SIS) nécessite un identifiant et un moyen d'authentification à deux facteurs. L'identifiant est généré par le SIS lors de la création du compte ou choisi par le client lors de l'inscription. L'identifiant est unique au sein du SIS, il ne peut être réutilisé par une autre entité ou porté vers un autre SIS ultérieurement. Le premier facteur d'authentification peut être un mot de passe, un code PIN ou un jeton (par exemple, un jeton OAuth). Pour les individus, le second facteur doit être biométrique. Pour les entités organisationnelles, logicielles ou matérielles, l'usage d'un certificat numérique est recommandé.

3.5.2 Administrateur

Les entités peuvent exercer des fonctions d'administration au sein d'un Système d'Information de Sûreté. La fonction d'Administrateur est par défaut exercée au moins par le responsable technique du SIS.

3.5.3 Modérateur

Certaines entités peuvent être désignées pour exercer des fonctions de modération au sein d'un Système d'Information de Sûreté. Elles sont promues par un Administrateur.

3.5.4 Utilisateur Vérifié

Une entité possède le statut "Vérifié" lorsque son identité et a été confirmée via des procédures administratives et techniques rigoureuses, telle que la validation de documents officiel.

3.5.5 Utilisateur Vérifié+

Les entités vérifiées sont éligibles au statut "Vérifié+" si elles exercent des professions liées aux services d'urgences. C'est par exemple le cas des professionnels de la santé, des secouristes et des agents de police.

3.5.6 Chaîne de confiance

La chaîne de confiance est un processus par lequel la confiance est établie et maintenant entre différents systèmes et entités. Elle repose sur la vérification cryptographique d'identités et permet de renforcer la sécurité des communications et l'authentification.

Dans le cadre du DEMP, un mécanisme vérifiant l'identité des entités et des Systèmes d'Information de Sûreté (SIS) permettrait de renforcer la chaîne de confiance en garantissant que les entités connectées au SIS sont connues et légitimes. Ce

mécanisme pourrait notamment passer le scannage mutuel de QR codes entre les entités et SIS (*Signal Messenger - Safety Numbers*; *GnuPG - Validating keys*).

3.5.7 Sécurité

La sécurité des communications, en particulier dans le contexte de la gestion des situations d'urgence, est fondamentale. La confidentialité, l'intégrité et la disponibilité des informations doit être garantie, de même que le respect de la vie privée. Le DEMP définie des directives générales en matière sécurité de l'information.

3.5.7.1 Chiffrement élémentaire

La transmission et la réception de données entre les Systèmes d'information de Sûreté (SIS) et les entités, ainsi qu'entre les SIS eux-mêmes doivent être sécurisées au moyen d'un canal SSL/TLS. Hors contexte de développement, ces échanges doivent être systématiquement chiffrés afin de renforcer la confidentialité et l'intégrité des échanges.

3.5.7.2 Chiffrement bout en bout

Le chiffrement bout en bout (E2EE pour End-to-End Encryption) est une méthode de sécurisation des communications caractérisée par le chiffrement des échanges dès leur émission et jusqu'à leur réception. Ce type de chiffrement garantit que seul l'émetteur et le destinataire légitime puissent accéder au contenu des messages échangés, et que ces derniers n'ont pas été manipulés ou altérés durant leur transfert.

Malgré ses avantages en termes de sécurité, le chiffrement bout en bout présente des contraintes techniques tels qu'un usage accru de ressources systèmes, en particulier sur les appareils utilisés pour communiquer avec le Système d'Information de Sûreté (facteur qui peut être critique dans le cadre de la gestion des situations d'urgence) ainsi que des problèmes de compatibilité et d'accès aux données chiffrées en cas de mise à jour logicielle ou changement de matériel.

En outre, le chiffrement bout en bout peut être soumis à des contraintes juridiques dans certains territoires, notamment en raison de réglementations sur la surveillance des télécommunications, ce qui réduit drastiquement son rapport coût-bénéfice.

L'implémentation du chiffrement bout en bout est considérée comme optionnelle dans le cadre du DEMP et son utilisation doit être considérée avec précaution.

3.5.8 Accessibilité

L'accessibilité est un aspect important du protocole DEMP. Elle vise à assurer que l'ensemble des utilisateurs, quelle que soit leur situation, puissent accéder aux fonctionnalités et informations transmises par le Système d'Information de Sûreté (SIS).

3.5.8.1 Inclusion

Les clients implémentant le protocole DEMP doivent fournir une expérience utilisateur inclusive et responsive, permettant notamment aux personnes en situation de handicap visuel, auditif ou cognitif de pouvoir utiliser l'application dans de bonnes conditions et en tenant compte des normes d'accessibilité existantes (Initiative (WAI)).

3.5.8.2 Adaptabilité

L'implémentation des clients doit prendre en considération les conditions dans lesquelles les appareils pourraient être utilisés dans le cas d'une situation d'urgence.

De manière générale, les situations d'urgence peuvent se produire dans des environnements exposés à des conditions particulièrement contraignantes, voir extrêmes, notamment en termes de bruit, éclairage, conditions météorologiques ou mouvements. Une attention particulière doit être apportée à l'expérience utilisateur dans ces conditions. Par ailleurs l'usage des ressources systèmes des appareils doit être optimisé afin de prévenir un usage intensif du matériel pouvant conduire à une décharge rapide, à une dégradation critique des performances ou défaillance logicielle.

De plus, au cours d'une situation d'urgence, les personnes blessées ou en situation de stress intense peuvent voir leurs facultés physiques et cognitives diminuées. L'implémentation des clients DEMP doivent tenir compte de ces facteurs et fournir une expérience utilisateur aussi simple, intuitive et épurée que possible.

3.5.8.3 Internationalisation

Le protocole DEMP encourage l'intégration d'un support multilingue pour garantir que les utilisateurs puissent accéder aux informations dans leur langue maternelle. Les clients DEMP doivent être capables de détecter et de s'adapter automatiquement à la langue préférée et l'environnement linguistique de l'utilisateur, tout en offrant la possibilité de personnaliser manuellement ces paramètres si nécessaire.

4. Application OASIS

OASIS (Open Alert and Safety Information System) est un prototype application dédié à la sécurité personnelle (personal safety). L'objectif principal de ce prototype est de démontrer les concepts fondamentaux du DEMP, à savoir le fonctionnement de l'Alerte Ouverte et du Système d'Information de Sûreté.

OASIS permet d'expérimenter et d'évaluer l'efficacité du DEMP dans les conditions proches du réel afin de d'exposer les particularités et le potentiel pratique du protocole. Bien que ce prototype ait essentiellement valeur de preuve de concept, il représente une étape nécessaire et essentielle à la poursuite du projet.

4.1 Analyse de l'existant

Afin de contextualiser le développement de l'application OASIS, il est nécessaire d'examiner les solutions existantes dans le domaine de la gestion des situations d'urgence. En Suisse, il existe quelques applications mobiles permettant de gérer des situations d'urgence, notamment AlertSwiss, MeteoSwiss, EchoSOS, Rega et Premiers Secours (IRFC).

AlertSwiss est l'application officielle de la Confédération pour la gestion des crises majeures. Elle diffuse des alertes en cas de situation d'urgence de grande ampleur (*Are you safe?*).

MeteoSwiss est l'application officielle de l'Office fédéral de météorologie et de climatologie (MétéoSuisse). Outre les bulletins météos, elle diffuse des alertes en cas de risque météorologique avéré (*MeteoSwiss-App - MeteoSchweiz*).

Rega (de l'organisation de sauvetage éponyme) est une application permettant d'alerter la centrale d'intervention et de transmettre sa géolocalisation en cas d'incident (Rega 2023).

EchoSOS est une application de gestion d'urgence permettant de contacter les services d'urgence, de transmettre sa géolocalisation et d'obtenir des conseils médicaux (*EchoSOS* | *Die Notfall-App* 2021).

Premiers Secours est l'application de la Croix-Rouge destinée à gérer les urgences médicales. Elle fournit des informations et directives à adopter en attendant l'arrivée de secouristes professionnels (*Premiers secours: une nouvelle application pour mieux réagir* 2023).

Tableau 18 : Comparatif des principales applications d'urgence suisses

Fonctionnalité	**SA**	**MS**	**Rega**	**EchoSOS**	**PS**
Diffusion d'alertes	Oui	Oui	Non	Non	Non
Usage de la géolocalisation	Oui	Oui	Oui	Non	Oui
Directives et conseils centralisés	Oui	Oui	Oui	Oui	Oui
Contact des services d'urgence	Non	Non	Oui	Oui	Oui
Support transfrontalier	Non	Non	Oui	Oui	Non
Décentralisation	Non	Non	Non	Non	Non

Les applications comparées, bien qu'opérationnelles dans leurs domaines respectifs, présentent des limitations significatives. Si AlertSwiss et MeteoSwiss diffusent des alertes géolocalisées, elles ne présentent aucune forme d'interopérabilité et pourraient s'avérer, par exemple, redondantes en cas de phénomène météo extrême. L'application Rega, bien que spécialisée dans les sauvetages aériens, demeure limitée à un usage très spécifique et lié à la centrale d'intervention de l'organisation. Enfin, EchoSOS fournit essentiellement des conseils et se démarque par la mise en relation des utilisateurs avec son réseau de partenaires santé. L'ensemble de ces applications s'appuie sur une approche centralisée.

À l'international, une étude menée au Royaume-Uni (Ford et al. 2022), portant sur l'usage des applications de sécurité personnelle dans la prévention des violences domestiques, a répertorié plus de 500 applications mobiles de gestion d'urgence sur les principaux magasins d'applications mobiles. La conclusion de cette étude suggère que les utilisateurs ont un avis mitigé sur ces applications car elles ne répondent pas aux attentes et leur utilisation peut être, dans certains cas, détournée. L'étude suggère également que le développement de telles applications devrait être régulé et sujet à des accréditations afin d'en garantir leur fiabilité.

La comparaison des applications d'urgence existantes, tant en Suisse qu'à l'international, met en évidence leurs limitations techniques en termes de fonctionnalités et d'interopérabilité et surtout leur incapacité à promouvoir une approche décentralisée favorisant l'autonomie et l'entraide communautaire. Ces faiblesses soulignent la nécessité de concevoir des applications répondant à une approche nouvelle comme celle du DEMP.

4.2 Choix technologiques

Le développement du prototype d'application OASIS repose sur une série de choix technologiques stratégiques. Ces choix sont essentiels pour assurer que l'application puisse répondre aux spécifications du DEMP.

4.2.1 Architecture

L'application est structurée autour d'une architecture client-serveur décentralisée où les entités et les Systèmes d'Information de Sûreté interagissent via un réseau distribué. Chaque instance de l'application est conçue pour fonctionner de manière autonome tout en étant capable de fonctionner en fédération avec d'autres membres du réseau si nécessaire.

4.2.2 Infrastructure

Le choix de l'infrastructure de communication et de partage d'informations est l'un des choix les plus importants car il doit être en adéquation avec l'ensemble des recommandations stratégiques, conceptuelles et techniques du DEMP.

4.2.2.1 Exigences

4.2.2.1.1 Décentralisation

L'infrastructure doit permettre une gestion décentralisée des communications et du partage d'informations **afin d'éviter tout point de défaillance unique** en garantissant la continuité des activités en cas d'indisponibilité d'un serveur, d'une instance de Système d'Information de Sûreté (SIS) ou d'une partie du réseau.

4.2.2.1.2 Interopérabilité

L'infrastructure doit être capable de communiquer et d'interagir avec les autres Systèmes d'Information de Sûreté (SIS) sans entrave de nature technique telles que des configurations réseaux ou des environnements linguistiques hétérogènes.

4.2.2.1.3 Sécurité

L'infrastructure doit répondre à des exigences élémentaires en matière de confidentialité, d'intégrité et de disponibilité en garantissant le chiffrage des canaux de communication entre les entités, les Systèmes d'Information de Sûreté (SIS) et les serveurs de stockage de données. Des mesures de restrictions d'accès techniques doivent être disponibles et mises en œuvre afin d'exclure tout accès indu à un service découlant directement ou indirectement de l'infrastructure.

4.2.2.1.4 Scalabilité

L'infrastructure doit être en mesure de s'adapter à tout moment et sans interruption à une augmentation significative de l'activité ou du volume d'informations échangées, sans que cela compromettre les performances, la sécurité ou la disponibilité.

4.2.2.1.5 Administration

L'infrastructure doit disposer d'outils permettant la surveillance continue et l'audit de l'état du système et du réseau afin de pouvoir anticiper ou répondre à des potentiels incidents techniques. Des mesures de sauvegarde et restauration, de réplication et de redondance doivent pouvoir être mises en œuvre et testés ponctuellement.

4.2.2.1.6 Technologies libres

L'infrastructure doit s'appuyer sur des technologies et logiciels sous licence libres pour garantir la transparence du système, faciliter les audits de sécurité et encourager le retour d'expérience et l'innovation communautaire, conformément à l'esprit du DEMP.

4.2.3 Solutions

Pour répondre aux exigences techniques définies par le DEMP, deux technologies ont été retenues : **Matrix et XMPP.** Ces deux protocoles ouverts ont été retenus pour leur capacité à offrir une infrastructure décentralisée, interopérable, sécurisée, et scalables, en parfaite adéquation avec les objectifs du protocole DEMP.

4.2.3.1.1 XMPP

XMPP - Extensible Messaging and Presence Protocol (anciennement Jabber) est un protocole ouvert et destiné à la messagerie instantanée et plus généralement, au partage de données entre applications et systèmes hétérogènes de manière décentralisée. Techniquement, il s'agit d'une application XML permettant la transmission et la réception de données structurées et la gestion de la présence en quasi temp réel (Saint-Andre 2011).

Ce protocole a été initialement développé Jeremie Miller et la communauté open source en 1999 et encadré par la suite par un groupe de travail de l'IETF. XMPP est extensible et a, entre autres, été utilisé par Google, Facebook et Microsoft dans les années 2010, dans un effort d'innovation et d'interopérabilité entre les messageries instantanées Google Talk, Facebook Messenger et Skype. Ces initiatives ont été abandonnées entre temps mais XMPP poursuit son développement et il est encore très largement utilisé de nos jours pour toute sorte d'applications liées à l'échange de messages, allant du jeu en

ligne au transfert de fichiers en passant par la visioconférence ou la gestion d'objets connectés.

4.2.3.1.2 Matrix

Matrix est un protocole de communication ouvert et décentralisé, respectivement, une spécification (*Matrix Specification*), conçu pour la messagerie instantanée et la gestion de la présence, tout en permettant le partage de données en quasi-temps réel entre différentes plateformes, applications et systèmes. Techniquement, Matrix utilise JSON pour structurer et transporter les données. Son implémentation s'architecture autour d'un ensemble d'APIs RESTful et il inclue nativement des mécanismes de sécurité avancé tels que le chiffrement de bout en bout.

Matrix a été créé en 2014 par une équipe de développeurs de l'entreprise Amdocs, sous la direction de Matthew Hodgson et Amandine Le Pape, avant de devenir un projet indépendant soutenu par la fondation à but non lucratif Matrix.org.

Matrix est souvent comparé à XMPP en raison de son objectif similaire de décentralisation et d'interopérabilité, mais il se distingue par sa conception centrée autour de technologies et concepts modernes.

4.2.3.2 Comparatif XMPP versus Matrix

Tableau 19 : Comparatif de XMPP et Matrix

Caractéristiques	**XMPP**	**Matrix**
Année de création	1999	2014
Format de données	XML	JSON
Décentralisation	Oui	Nativement)
Fédération de serveurs	Oui	Nativement
Chiffrement élémentaire (SSL/TLS)	Oui	Nativement
Chiffrement bout en bout (E2EE)	Oui	Nativement
Interopérabilité	Oui	Nativement
Synchronisation entre appareils	Oui	Nativement

Après avoir comparé XMPP et Matrix, il apparaît que Matrix répond incontestablement mieux aux exigences stratégiques et techniques définies par le DEMP. Le protocole Matrix, avec son architecture décentralisée et son support natif pour la fédération des serveurs, s'aligne parfaitement avec les exigences du DEMP.

4.3 Conception

La conception du prototype d'application OASIS a été guidée par un objectif principal, celui de démontrer la faisabilité de la mise en œuvre d'une infrastructure capable de supporter les fondamentaux du DEMP, à savoir :

- La communication et le partage d'informations en temps réel
- Les Systèmes d'Information de Sûreté (SIS)
- Les zones de sûreté
- Les entités et appareils
- **Les alertes**

Dans cette optique, la conception du prototype OASIS a été simplifiée au maximum. L'accent a été mis sur les fonctionnalités en privilégiant le développement de deux outils en ligne de commande : **oasis-cli** pour la gestion des composants des Systèmes d'Information de Sûreté (SIS) et **oasis-sim** pour évaluer le lancement d'alertes ouvertes dans un environnement proche de la réalité.

4.4 Développement

Chaque décision technologique, qu'il s'agisse de la sélection du langage de programmation, des bibliothèques utilisées, ou de l'architecture logicielle, a été prise avec précaution pour s'assurer que l'application réponde en premier lieu à son objectif de **preuve de concept pour la gestion des alertes ouvertes et des systèmes d'information de sûreté**.

Le développement du prototype a été guidé par une approche pragmatique, modulaire et reproductible. L'objectif était de pouvoir installer, comprendre et tester rapidement les concepts clés du DEMP.

4.4.1.1 Langage de programmation

Le langage Python a été choisi pour l'ensemble du développement en raison de sa simplicité, de ses bibliothèques standard et tierces ainsi que ses outils permettant de mettre en place rapidement un environnement de développement opérationnel.

4.4.1.2 Virtualisation

La plateforme Docker a été utilisée afin de paramétrer un environnement de développement containerisé, dans un effort de simplicité et de reproductibilité de la solution indépendamment du système d'exploitation.

4.4.1.3 Serveur Matrix

Synapse est l'implémentation coté serveur de référence de la spécification Matrix développé par la fondation éponyme. En 2023, le logiciel libre a été forké et il est désormais maintenu par la société Element.

4.4.1.4 Reverse Proxy

Nginx (*nginx*) est un serveur HTTP libre et flexible qui peut être utilisé en tant que reverse proxy afin de permettre l'accès au serveur Synapse depuis l'hôte locale ou directement depuis le Web. L'usage de Nginx en tant que reverse proxy est recommandé par la fondation Matrix car il facilite sa gestion et améliore la sécurité de l'infrastructure. En outre Nginx peut être utilisé comme load balancer afin de répartir le trafic sur plusieurs serveurs Synapse si nécessaire.

4.4.1.5 Composants tiers

4.4.1.5.1 SQLite

SQLite est une bibliothèque programmée en langage C offrant un système de gestion de bases de données relationnelles léger et embarqué (*SQLite Home Page*). Elle a été

utilisée par Synapse pour le stockage des données, notamment en raison de sa simplicité et de son absence de dépendances externes.

4.4.1.5.2 Nio

Nio (*matrix-nio/matrix-nio* 2024) est une bibliothèque Python offrant une interface client pour communiquer avec un serveur Matrix, elle est fondée sur la bibliothèque AsyncIO, permettant de faire de la programmation concurrente (*asyncio — Asynchronous I/O*). Elle a notamment été utilisée pour implémenter les agents autonomes OASIS et interagir avec Synape, néanmoins, elle ne prend pas (encore) en charge l'ensemble de la spécification Matrix. Pour réaliser les parties de l'application qui ne nécessitaient pas strictement une approche asynchrone, l'API REST du serveur Synapse a été directement utilisée avec la bibliothèque HTTP Requests (*Requests: HTTP for Humans™*).

4.5 Implémentation

L'implémentation du prototype a consisté à porter les concepts fondamentaux du DEMP en code source fonctionnel, testable et reproductible. L'objectif était de s'assurer que chaque fonctionnalité clé puisse être techniquement et objectivement validée dans un environnement de développement contrôlé.

4.5.1.1 Création de l'environnement de développement

La première étape consiste à installer Docker Engine et à configurer un environnement Python virtualisé, puis à élaborer les fichiers de configuration nécessaires pour l'installation des dépendances Python (**requirements.txt**) ainsi que pour le fonctionnement de Synapse (**homeserver.yaml**), Nginx (**default.conf)**. Ensuite un fichier de configuration **docker-compose.yaml doit être** créé pour orchestrer le déploiement de ces services en tant que conteneurs Docker. Enfin, le fichier **/etc/hosts** de l'hôte local doit être modifié afin d'ajouter le nom de domaine oasis.local, permettant ainsi un accès au(x) serveur(s) Synapse depuis l'extérieur des conteneurs avec l'application OASIS ou, à des fins de tests, avec un client Matrix quelconque tels que Element ou Cinny (*Clients*).

4.5.1.2 Accès Administrateur

Pour effectuer la plupart des tâches de gestion au sein d'OASIS et d'utiliser les outils en ligne de commande, il est nécessaire de s'authentifier en tant qu'Administrateur. Par défaut, les comptes administrateurs sont disponibles sur les trois Système d'Information de sûreté (SIS) de OASIS :

- SIS 1 : root@sis1.oasis.local
- SIS 2 : root@sis2.oasis.local
- SIS 3 : root@sis3.oasis.local

4.5.1.3 Outil en ligne de commande oasis-cli

L'outil en ligne de commande oasis-cli est au cœur de l'application OASIS. Il permet de paramétrer les différents composants du Système d'Information de Sûreté (SIS), notamment la configuration des entités, des appareils, des zones de sûreté, ainsi que la gestion des alertes et des paramètres de fédération.

4.5.1.4 Gestion des Systèmes d'Information de Sûreté

Le Système d'Information de Sûreté (SIS) a pour mission de gérer la collecte, le traitement et la distribution des données, tout en assurant la gestion des entités, des appareils et des zones de sûreté. Sur le plan technique, il représente à la fois les services Nginx, Synapse et le moteur de base de données utilisé pour le stockage des données SQLite.

Pour les besoins de l'application OASIS, trois SIS ont été créés. Afin que chacun d'entre eux puisse être atteint depuis l'hôte local, des ports de fonctionnement différents leur ont été attribués :

- Domaine SIS 1 : http://sis1.oasis.local:8000
- Domaine SIS 2 : http://sis2.oasis.local:8080
- Domaine SIS 3 : http://sis3.oasis.local:8888

Ces trois instances ont respectivement permis d'effectuer des tests de fédération des SIS et de propagation d'alertes ouvertes.

4.5.1.5 Gestion des zones de sûreté

Les zones de sûreté constituent des périmètres au sein du Système d'Information de Sûreté (SIS). Sur le plan technique, elles sont représentées par les rooms Matrix (*Matrix Specification*), auxquelles sont ajoutées des métadonnées spécifiques au DEMP.

OASIS permet de gérer des zones de sûreté grâce à l'outil en ligne de commande **oasis-cli**.

4.5.1.6 Gestion des entités et appareils

Les entités et appareils représentent les composants principaux au sein du Système d'Information de Sûreté. Les entités représentent des personnes, des organisations, des logiciels (agents autonomes) ou du matériel (objets connectés). Les appareils font

référence à des dispositifs logiciel ou matériel jouant un rôle passif ou actif au sein du SIS.

Dans la nomenclature Matrix, les entités correspondent à des comptes utilisateur tandis que les appareils correspondent à des “dispositifs” (devices). Dans les deux cas de figure, des métadonnées DEMP sont ajoutées à ces composants afin d’étendre leurs capacités.

4.5.1.7 Gestion des alertes

Les alertes sont des messages émis par le Système d’Information de Sûreté pour signaler une situation d’urgence, un événement important ou un avertissement. Sur le plan technique, les alertes sont gérées comme des messages Matrix diffusés dans les rooms associées, assortis de métadonnées DEMP permettant notamment de caractériser le type d’alerte et sa portée.

OASIS permet de gérer déclencher des alertes grâce à l’agent de test (TestAgent).

4.5.1.8 Agent d’Alerte

L’Agent d'Alerte (AlertAgent) est une entité logicielle chargée de gérer les événements (incluant les messages) envoyés par les autres entités dans une zone de sûreté. Concrètement, il s'agit d'un bot selon la spécification Matrix. L'Agent d'Alerte est généralement présent dans toutes les zones de sûreté de son Système d’Information de Sûreté (SIS) et peut également être invité dans des zones situées sur d'autres SIS dans le cadre d'une fédération DEMP.

OASIS permet de gérer des alertes grâce à l’agent d’alerte (AlertAgent).

4.5.1.9 Agent de Test

L’Agent de Test (TestAgent) est une entité logicielle permettant d’effectuer des tests tels que le déclenchement d’alertes. À l’instar de l’Agent d’Alerte, il s’agit techniquement d’un bot Matrix disposant de privilèges particuliers. L’Agent de Test est utilisé en arrière-plan par **oasis-sim** pour les simulations, mais peut également être démarré manuellement.

4.5.1.10 Agent de Surveillance

L’Agent de Surveillance (Monitoring Agent) est une entité logicielle chargée d’inspecter tous les événements qui se produisent au sein d’un Système d’Information de Sûreté (SIS), sur le plan technique, il s’agit également d’un bot Matrix.

OASIS permet de visualiser les événements du SIS grâce à l’agent d’alerte MonitoringAgent.

4.5.1.11 Agent Générique

L'Agent Générique (Generic Agent) est une entité logicielle chargée d'émuler le comportant d'une autre entité ou d'appareils. Il s'agit d'un bot Matrix capable d'interagir avec le Système d'Information de Sûreté (SIS) en transmettant des données "mock" à des fins de test.

OASIS permet de créer des entités fictives et de les activer grâce à l'agent générique GenericAgent.

4.5.1.12 Correspondance terminologique

Pour une meilleure compréhension du code source, le tableau suivant fournit une correspondance terminologique entre le DEMP et la spécification Matrix.

Tableau 20 : Correspondance terminologique DEMP / Matrix

DEMP	**Matrix**
Système d'Information de Sûreté (SIS)	Homeserver
Zone de sûreté	Room
Entité	Member
Appareil	Device
Métadonnées DEMP	State Events personnalisés

4.6 Simulation

La simulation se concentre sur l'évaluation de l'architecture du prototype d'application OASIS en mettant l'accent sur un concept fondamental du DEMP : l'Alerte Ouverte. Cette simulation vise à tester en conditions proches de la réalité la capacité de l'infrastructure, bâtie sur la spécification Matrix, à gérer la diffusion des alertes, la communication entre les entités et les zones de sûreté, ainsi que l'interopérabilité entre différents Systèmes d'Information de Sûreté (SIS). L'objectif final est de valider la viabilité technique tout en identifiant d'éventuelles limitations ou axes d'amélioration pour de futurs développements.

4.6.1 Environnement de test

Pour garantir l'intégrité et la fiabilité des résultats, chaque simulation est exécutée dans des conteneurs distincts, systématiquement recréés avant l'exécution des tests et réinitialisés. Le script d'initialisation lance les services requis et les préconfigurent avec le compte Administrateur ainsi que les agents autonomes AlertAgent, MonitoringAgent, TestAgent et GenericAgent. Toute donnée superflue ou état du système préexistant sont

exclus afin d'éviter les effets de bord et ainsi garantir au mieux un environnement propre et reproductible pour chaque test.

4.6.2 Outil en ligne de commande oasis-sim

L'outil en ligne de commande **oasis-sim** a été conçu pour tester et évaluer le comportement de l'architecture OASIS dans le cadre du lancement d'alertes ouvertes DEMP. S'appuyant en grande partie sur les fonctionnalités de oasis-cli, oasis-sim automatise la création et l'exécution d'environnement simulés complexes en permettant notamment de paramétrer finement les entités, les zones de sûreté et les alertes.

4.6.3 Test de l'alerte de zone

Cette première simulation se concentre sur l'envoi et la gestion d'une **alerte de zone**. Une alerte de zone DEMP se limite à la zone de sureté dans laquelle elle a été déclenchée. Ce test vise à évaluer la capacité de l'Agent d'Alerte à notifier toutes les entités présentes dans la zone. La simulation recrée un scénario réaliste dans lequel une urgence survient dans une zone de sûreté définie, permettant ainsi de valider la réactivité du système et la gestion des événements en temps réel.

4.6.3.1 Objectif

L'objectif de ce test est de valider la capacité du Système d'Information de Sûreté (SIS) à propager une alerte en temps réel dans une zone de sûreté et de recevoir une confirmation de réception de la part de toutes les entités présentes.

4.6.3.2 Initialisation

Le simulateur effectue les opérations suivantes d'initialisation de l'environnement de test :

- Création d'une zone de sûreté étiquetée Alpha sur le domaine SIS N°1.
- Ajout des agents autonomes AlertAgent, (Agent d'alerte) TestAgent (Agent de test) MonitorAgent (Agent de surveillance) dans la zone de sûreté.
- Création de trois GenericAgent (Alice, Bob et Mallory) sur SIS 1.
- Ajout de Alice, Bob et Mallory dans la zone de sûreté Alpha.
- Activation de AlertAgent, TestAgent et tous les GenericAgent.
- Activation de MonitoringAgent sur l'hôte local pour visualiser la journalisation en temps réel.

4.6.4 Exécution

Le simulateur ordonne à l'agent autonome **TestAgent** de déclencher une alerte de type **ch.demp.alert.type.test** (alerte de test) avec une visibilité de type **ch.demp.alert.visibility.zone** (alerte de zone). Après 10 secondes, le simulateur

désactive tous les agents autonomes (à l'exception de **MonitoringAgent**, activé manuellement sur l'hôte local) et termine la simulation.

L'alerte est déclenchée et propagée dans la zone de sûreté. **AlertAgent** envoie un signal **ch.demp.command.poke** à chaque entité figurant dans la zone de sûreté. Les entités présentes (en ligne) dans la zone de sûreté répondent automatiquement à l'agent d'alerte par le même signal. Cela permet à ce dernier d'indexer les entités qui sont effectivement actives dans la zone de sûreté au moment du déclenchement de l'alerte.

Dans un second temps, **AlertAgent** effectue une demande de confirmation de réception de l'alerte auprès de chaque entité présente. Les entités logicielles génériques **Alice**, **Bob** et **Mallory** confirment la réception auprès de **AlertAgent**.

MonitoringAgent, l'agent autonome de surveillance, a journalisé l'ensemble des interactions intervenues durant l'alerte et le résultat de la simulation est **conforme aux attentes**.

Le test a été répété 3 fois de suite. Un **diagramme de séquence** des opérations est fourni en Annexe 2.

4.6.5 Test de l'alerte système

Cette deuxième simulation a pour objectif d'évaluer une **alerte système**. Ce type d'alerte DEMP, destiné aux événements d'envergure moyenne à considérable, a pour objectif de diffuser une alerte à l'ensemble des zones de sûreté d'un Système d'Information de Sûreté (SIS). Contrairement à l'alerte de zone, l'alerte système doit être propagée à l'échelle globale du SIS. La simulation recrée un scénario dans lequel un incident est susceptible d'impacter plusieurs zones.

4.6.5.1 Objectif

L'objectif de ce test est de valider la capacité du Système d'Information de Sûreté (SIS) à propager une alerte en temps réel à l'ensemble de ses zones de sûreté.

4.6.5.2 Initialisation

Le simulateur effectue les opérations suivantes d'initialisation de l'environnement de test :

- Création de trois zones de sûreté **Alpha, Beta, Gamma** sur le domaine **SIS 1**.
- Ajout des agents autonomes **AlertAgent**, (Agent d'alerte) **TestAgent (**Agent de test) **MonitorAgent** (Agent de surveillance) dans la zone de sûreté **Alpha**.
-

- Création de trois GenericAgent (Alice, Bob, Mallory) sur SIS 1.
- Ajout de Alice dans la zone de sûreté Alpha.
- Ajout de Bob dans la zone de sûreté Beta.
- Ajout de Mallory dans la zone de sûreté Gamma.
- Activation de AlertAgent, TestAgent et tous les GenericAgent.
- Activation de MonitoringAgent sur l'hôte local pour visualiser la journalisation en temps réel.

4.6.5.3 Exécution

Le simulateur ordonne à l'agent autonome **TestAgent** de déclencher une alerte de type **ch.demp.alert.type.test** (alerte de test) avec une visibilité de type **ch.demp.alert.visibility.system** (alerte système) depuis la zone de sûreté **Alpha**. Après 10 secondes, le simulateur désactive tous les agents autonomes (à l'exception de **MonitoringAgent**, activé manuellement sur l'hôte local) et termine la simulation.

L'alerte est déclenchée depuis la zone **Alpha** et propagée simultanément aux zones **Beta** et **Gamma**. **AlertAgent** envoie un signal **ch.demp.command.poke** à chaque entité figurant dans chaque zone de sûreté. Les entités présentes (en ligne) dans chaque zone de sûreté répondent automatiquement à l'agent d'alerte par le même signal. Cela permet à l'agent d'alerte d'indexer les entités qui sont effectivement actives dans la zone de sûreté au moment où l'alerte est déclenchée.

Dans un second temps, **AlertAgent** effectue une demande de confirmation de réception de l'alerte auprès de chaque entité présente. **Alice**, **Bob** et **Mallory** situées respectivement dans les zones **Alpha**, **Beta** et **Gamma**, confirment la réception auprès de l'agent d'alerte.

MonitoringAgent, l'agent autonome de surveillance, a journalisé l'ensemble des interactions intervenues durant l'alerte et le résultat de la simulation est **conforme aux attentes**.

Le test a été répété 3 fois de suite. Un **diagramme de séquence** des opérations est fourni en Annexe 3.

4.6.6 Test de l'alerte fédérée

Cette troisième simulation se focalise sur l'usage d'une **alerte fédérée**. Ce type d'alerte DEMP se prédestine aux événements majeurs puisqu'il s'agit de diffuser une alerte à plusieurs Systèmes d'Information de Sûreté (SIS) simultanément. Ces SIS peuvent être répartis géographiques et contenir de des milliers d'entités chacun. La simulation recrée

un scénario dans lequel un événement majeur s'est produit et implique une réponse de grande envergure, impliquant différentes institutions.

4.6.6.1 Objectif

L'objectif de ce test est de valider la capacité du Système d'Information de Sûreté (SIS) à propager une alerte en temps réel à un autre SIS fédéré.

4.6.6.2 Initialisation

Le simulateur effectue les opérations suivantes d'initialisation de l'environnement de test :

- Création d'une zone de sûreté Alpha sur le SIS 1.
- Création d'une zone de sûreté Beta sur le SIS 2.
- Ajout d'Alice dans la zone de sûreté Alpha du SIS 1.
- Ajout de Bob dans la zone de sûreté Beta du SIS 2.
- Ajout de AlertAgent du SIS 1 dans la zone Alpha du domaine SIS 1.
- Ajout de AlertAgent du SIS 2 dans la zone Alpha du domaine SIS 1.
- Activation de tous les agents.
- Activation de MonitoringAgent sur l'hôte local pour visualiser la journalisation en temps réel.

4.6.6.3 Exécution

Le simulateur ordonne à l'agent autonome **TestAgent** de déclencher une alerte de type **ch.demp.alert.type.test** (alerte de test) avec une visibilité de type **ch.demp.alert.visibility.federated** (alerte fédérée) depuis la zone de sûreté **Alpha** du SIS 1. L'alerte est déclenchée depuis la zone **Alpha** du SIS 1. **AlertAgent** du **SIS 2**, présent dans la zone **Alpha** du SIS 1, envoie un signal **ch.demp.command.forward** à **AlertAgent** du SIS 1 et transfère l'alerte avec le signal **ch.demp.alert.type.system** à **SIS 2**. Cela signifie que toutes les zones du **SIS 2** reçoivent l'alerte déclenchée dans la zone Alpha du **SIS 1**, en l'occurrence, seule la zone **Beta** reçoit l'alerte, car il n'y a qu'une seule zone sur le **SIS 2**.

Parallèlement un signal **ch.demp.command.poke** est envoyé par les deux AlertAgent à toutes les entités actives figurant dans chaque zone de sûreté. Les entités présentes (en ligne) dans chaque zone de sûreté répondent automatiquement à l'agent d'alerte par le même signal.

Dans un second temps, les **AlertAgent** effectue une demande de confirmation de réception de l'alerte auprès de chaque entité présente, dans leur SIS respectifs. **Alice**,

Bob situées dans les zones Alpha du SIS 1 et Beta du SIS 2, confirment la réception auprès de l'agent d'alerte.

Après 10 secondes, le simulateur désactive tous les agents autonomes (à l'exception de **MonitoringAgent**, activé manuellement sur l'hôte local) et termine la simulation.

Le test a été répété 3 fois de suite. Un **diagramme de séquence** des opérations est fourni en Annexe 4.

4.6.7 Test de l'Alerte ouverte

Cette quatrième et dernière simulation concerne la propagation d'une **alerte ouverte**. L'alerte ouverte DEMP a pour objectif de permettre la propagation d'une alerte aux SIS fédérés et de permettre à ceux-ci de propager automatiquement l'alerte au-delà de la fédération. Ce test de simulation vise à évaluer la capacité de OASIS à propager une telle alerte. En effet, contrairement aux autres types d'alertes, une alerte ouverte n'est pas limitée par les frontières des zones, des SIS ou d'une fédération, elle a théoriquement une portée globale et illimitée. La simulation recrée un scénario où une situation d'urgence désespérée nécessite une alerte d'urgence globale.

4.6.7.1 Objectif

L'objectif de ce test est de valider la capacité du Système d'Information de Sûreté (SIS) à propager une Alerte Ouverte.

4.6.7.2 Initialisation

Le simulateur effectue les opérations suivantes d'initialisation de l'environnement de simulation :

- Création d'une zone de sûreté Alpha sur le SIS 1.
- Création d'une zone de sûreté Beta sur le SIS 2.
- Création d'une zone de sûreté Gamma sur SIS 3.
- Ajout d'Alice dans la zone de sûreté Alpha du SIS 1.
- Ajout de Bob dans la zone de sûreté Beta du SIS 2.
- Ajout de Mallory dans la zone de sûreté Gamma du SIS 3.
- Ajout de AlertAgent du SIS 1 dans la zone Alpha du domaine SIS 1.
- Ajout de AlertAgent du SIS 2 dans la zone Alpha du domaine SIS 1.
- Ajout de AlertAgent du SIS 3 dans la zone Beta du domaine SIS 2.
- Activation de tous les agents.
- Activation de MonitoringAgent sur l'hôte local pour visualiser la journalisation en temps réel.

4.6.7.3 Exécution

L'Alerte Ouverte est déclenchée depuis la zone **Alpha** du **SIS 1**. **AlertAgent** du **SIS 2**, présent dans la zone **Alpha** du **SIS 1**, dans le cadre d'une fédération, envoie un signal **ch.demp.command.forward** à **AlertAgent** du **SIS 1** et transfère l'alerte avec le signal **ch.demp.alert.type.system** à **SIS 2**. Cela signifie que toutes les zones du **SIS 2** reçoivent l'alerte déclenchée dans la zone Alpha du **SIS 1**, en l'occurrence, seule la zone **Beta** reçoit l'alerte, car il n'y a qu'une seule zone sur le **SIS 2**. Le **AlertAgent** du **SIS 3** est présent dans la zone **Beta** de **SIS 2**. Comme il n'est pas en fédération avec **SIS 1**, l'alerte ne le concerne pas directement, cependant, étant donné qu'il s'agit d'une alerte ouverte, il peut soit l'ignorer, soit la traiter. Il choisit de la traiter, et émet à son tour un signal **ch.demp.command.forward,** suivit d'une alerte système sur **SIS 3**.

Parallèlement un signal **ch.demp.command.poke** est envoyé par les tous les AlertAgent à toutes les entités actives dans leur zone de sûreté respectives. Les entités présentes (en ligne) dans chaque zone de sûreté répondent automatiquement à l'agent d'alerte par le même signal.

Dans un second temps, tous les **AlertAgent** effectuent une demande de confirmation de réception de l'alerte auprès de chaque entité présente, dans leur SIS respectifs. **Alice** située dans les zones **Alpha** du **SIS 1**, confirme la réception. **Bob**, situé dans la zone **Beta**, confirme l'alerte, enfin **Mallory**, situé dans la zone **Gamma** de **SIS 3**, confirme également la réception de l'alerte.

MonitoringAgent, l'agent autonome de surveillance, a journalisé l'ensemble des interactions intervenues durant l'alerte et le résultat de la simulation est **conforme aux attentes**.

Le test a été répété 3 fois de suite. Un **diagramme de séquence** des opérations est fourni en Annexe 5.

4.6.8 Évaluation de l'alerte de zone

La simulation de l'alerte de zone devait répondre aux 5 points suivants :

- Déclenchement de l'alerte (ch.demp.alert.start)
- Envoi des poke de présence (ch.demp.command.poke)
- Réponse aux poke de toutes les entités présentes.
- Demande de confirmation de réception de l'alerte (ch.demp.command.confirm)
- Accusé de réception toutes les entités présents (ch.demp.command.poke)

Dans le premier test, l'agent de test (TestAgent) a correctement déclenché le l'alerte, tandis que l'agent d'alerte (AlertAget) a ffectué un poke de présence à destination de toutes les entités présentes dans la zone de sûreté. l'AlertAgent n'a toutefois pas envoyé de demande de confirmation de réception aux entités. **Le score de ce test est de 2/5**.

Dans le second test, l'AlertAgent a correctement déclenché l'alerte et envoyé les poke de présence, auxquelles les entités ont répondu. Il a ensuite envoyé une demande de confirmation de réception de l'alerte, à laquelle les entités n'ont pas répondu. **Le score de ce test est de 3/5**.

Dans le dernier test, l'AlertAgent a correctement déclenché l'alerte, effectué les poke de présence et les demandes de confirmation. Toutes les entités ont répondu à la demande de confirmation. Ce troisième test est conforme aux attentes. **Le score de ce test est de 5/5**.

Le taux de réussite de cette simulation est de 66%. Les données brutes des tests sont disponibles en Annexe 6.

4.6.9 Évaluation de l'alerte système

La simulation de l'alerte système devait répondre aux 6 points suivants :

- Déclenchement de l'alerte (ch.demp.alert.start)
- Propagation de l'alerte dans toutes les zones de sûreté (Alpha et Beta et Gamma)
- Envoi des poke de présence (ch.demp.command.poke) à Alice, Bob et Mallory.
- Réponse aux poke de Alice, Bob et Mallory.
- Demande de confirmation (ch.demp.command.confirm)
- Accusé de réception de Alice, Bob et Mallory.

Dans le premier test, le l'agent de test (TestAgent) a correctement déclenché l'alerte dans les zones Alpha et Beta, mais pas Gamma. L'agent d'alerte (AlertAgent) a effectué un poke de présence à destination de Alice et Bob, mais pas Mallory. Ces derniers ont toutefois répondu. Il a également effectué des demandes de confirmation uniquement à Alice et Bob, qui ont également accusé de réception. **Le score de ce test est de 2/6**.

Dans le second test, le TestAgent a correctement déclenché l'alerte dans les zones Alpha, Beta et Gamma. Il a effectué avec succès les poke de présence et demande de confirmation, auxquelles les entités ont répondu correctement. **Le score de ce test est de 6/6**.

Dans le dernier test, le TestAgent a correctement déclenché l'alerte. L'Agent d'alerte a effectué les poke de présence correctement, mais seul Bob a répondu. **Le score de ce test est de 1/6**.

Le taux de réussite de cette simulation est de 50%. Les données brutes des tests sont disponibles en Annexe 6.

4.6.10 Évaluation de l'alerte fédérée

La simulation de l'alerte fédérée devait répondre aux 7 points suivants :

- Déclenchement de l'alerte (ch.demp.alert.start)
- Envoi de poke de présence (ch.demp.command.poke)
- Réponse des entités présentes.
- Transfère de l'alerte sur le Système d'Information de Sûreté (SIS) fédéré (ch.demp.command.forward)
- Déclenchement de l'alerte initiale sous forme d'alerte système sur le SIS fédéré.
- Demande de confirmation de réception de l'alerte.
- Accusé de réception des entités présentes.

Dans le premier test, le l'agent de test (TestAgent) a correctement déclenché l'alerte dans les zones Alpha du domaine SIS 1. L'agent d'alerte (AlertAgent) du domaine SIS a correctement envoyé un signal de transfère et propagé l'alerte en tant qu'alerte système sur le domaine SIS 2. Effectué un poke de présence à destination de Alice et Bob, mais pas Mallory. Enfin, l'AlertAgent du domaine SIS 2 a également effectué les poke de présence et demande de confirmation auprès des entités présentes, seul Bob a répondu. L'AlertAgent du domaine SIS aurait dû effectuer les poke de présence et demandes de confirmation pour les entités présentes dans sa zone, et non l'AlertAgent de l'autre SIS. **Le score de ce test est de 4/7**.

Dans le second test, l'agent de test (TestAgent) déclenche l'alerte. L'agent d'alerte (AlertAgent) du domaine SIS 2, transfère correctement l'alerte sous forme d'alerte système dans son SIS mais encore une fois, ce même il s'occupe de tous les poke de présence et demande de confirmation, auxquels les entités ont répondu. **Le score de ce test est de 5/7**.

Dans le dernier test, l'agent de test (TestAgent) déclenche l'alerte, l'agent d'alerte du domaine SIS 2 transfère et propage l'alerte à son SIS correctement, puis il envoie des poke de présence et semble à nouveau envoyer un signal de transfère et de déclenchement d'alerte, **le score de ce test est de 2/7**.

Le taux de réussite de cette simulation est de 52%. Les données brutes des tests sont disponibles en Annexe 6.

4.6.11 Évaluation de l'alerte ouverte

La simulation de l'alerte ouverte devait répondre aux points suivants :

- Déclenchement de l'alerte (ch.demp.alert.start)
- Envoi de poke de présence (ch.demp.command.poke)
- Réponse des entités présentes (ch.demp.command.poke).
- Transfère de l'alerte sur les deux autres Systèmes d'Information de Sûreté (SIS) (ch.demp.command.forward).
- Propagation de l'alerte initiale en alerte système sur les autres SIS. (ch.demp.alert.system)
- Demande de confirmation de réception de l'alerte (ch.demp.command.confirm).
- Accusé de réception des entités présentes (ch.demp.command.confirm).

Dans le premier test, l'agent de test (TestAgent) déclenche l'alerte. Elle est transférée par l'agent d'alerte du domaine SIS 1 (sans raison apparente) et du domaine SIS 2. Les agents d'alerte effectuent correctement les poke de présence dans leur SIS respectifs, auxquels les entités répondent correctement. Il n'y a néanmoins pas de demande confirmation effectuée ni de propagation de l'alerte pas le domaine SIS 3. **Le score de ce test est de 3/7**.

Dans le second test, l'agent de test (TestAgent) déclenche l'alerte. Elle est transférée par les agents d'alerte (AlertAgent) des domaines SIS 2 et 3, qui propagent ensuite l'alerte correctement dans leur SIS respectif, dans toutes les zones disponibles. Les poke de présence et demandes de confirmations sont conformes aux attentes. Seul bémol, l'AlertAgent du domaine SIS 1 a émis un signal de transfère de l'alerte à son propre SIS, à tort. **Le score de ce test est de 5/6**.

Dans ce troisième et dernier test l'alerte est correctement déclenchée par l'agent de test, les poke de présence et demande de confirmation sont réalisées correctement de part et d'autre des systèmes d'information de sûreté, il manque toutefois les signaux de transfère et de propagation de l'alerte. Le score de ce test est de 3/6.

Le taux de réussite de cette simulation est de 52%. Les données brutes des tests sont disponibles en Annexe 6.

4.6.12 Analyse des résultats

Avec un **taux de réussite global de 55%**, les résultats des tests ont été **conformes aux attentes dans plus de la moitié des cas**. Néanmoins des problèmes de fiabilité importants subsistent dans la gestion des alertes par OASIS. En particulier en ce qui concerne la propagation des alertes entre les différentes zones de sûreté et Systèmes d'Information de Sûreté (SIS). Une analyse plus approfondie des logs et des comportements observés durant les tests semble indiquer que ces problèmes émanent de possibles "race conditions" inhérentes à l'environnement concurrent dans lequel les entités sont amenées à interagir.

Par ailleurs, Synapse impose, entre autres, des quotas (*Configuration Manual - Synapse*) de messages par seconde afin de prévenir les dénis de service ou la propagation de messages non sollicités, bien qu'une partie de ces quotas puissent être paramétrés, cela ne semble rien arranger. La problématique est d'ailleurs évoquée ponctuellement par la communauté d'utilisateurs de Synapse, et seules des mesures contournement semblent être proposées. Enfin, il n'est pas exclu que l'implémentation de OASIS soit en cause, au moins dans une certaine mesure. De même que l'environnement de virtualisation ou les ressources systèmes utilisés pour exécuter les simulations.

Les données brutes des tests sont disponibles en Annexe 6.

4.6.13 Points d'amélioration

4.6.13.1 Analyse de code

Analyser et optimiser le code de l'application pour minimiser les risques de conditions de course, notamment en identifiant et en corrigeant les zones critiques où ces problèmes sont susceptibles de se produire.

4.6.13.2 Ajustement des quotas

Réexaminer les paramètres de quotas de messages par seconde imposés par Synapse, en tenant compte des besoins spécifiques du système OASIS, et tester des configurations alternatives pour trouver un équilibre entre sécurité et performance.

4.6.13.3 Audit

Analyser directement les fichiers journaux (logs) du serveur Synapse au lieu de capturer les événements avec une entité logicielle (MonitoringAgent). De cette manière, l'état du système peut être inspecté plus minutieusement et indépendamment de l'environnement d'exécution.

Conclusion

Ce mémoire a exploré la conception, le développement et l'implémentation du protocole de gestion d'urgence décentralisé DEMP. Son objectif principal était de démontrer la faisabilité technique d'un système capable de gérer efficacement les déclenchements d'alertes d'urgence dans un environnement décentralisé et digitalisé, tout en abordant les défis spécifiques liés à l'interopérabilité, la réactivité, et l'interconnexion des systèmes d'information.

Le prototype d'application OASIS, conçu comme une preuve de concept, a validé l'architecture du DEMP, en particulier l'un de ses concepts fondamentaux : l'alerte ouverte. Bien que les simulations réalisées aient montré des résultats contrastés, principalement en raison des limitations de l'infrastructure et de l'implémentation, les avancées obtenues ont permis d'identifier des pistes d'amélioration claires pour faire évoluer l'application OASIS en une véritable solution de sécurité personnelle.

Ce travail de Bachelor représente par ailleurs une étape importante pour le DEMP, ouvrant la voie à de futurs collaborations et à l'élaboration concrète d'un standard reconnu et adopté qui permettra non seulement de développer des solutions de pointe, mais contribuera également à digitaliser la gestion des urgences, à promouvoir l'entraide en temp de crise et à changer en profondeur la manière dont le public perçoit et conçoit la sécurité au quotidien.

J'ai la conviction que ce travail peut contribuer à préserver des vies en rendant la gestion des urgences plus rapide et accessible à tous. En intégrant des technologies innovantes dans des processus décentralisés de gestion, il est non seulement possible d'améliorer la réactivité face aux situations d'urgence mais aussi de bâtir des réseaux de solidarité renforcés par une technologie qui place l'humain et la communauté au cœur de la sécurité. Le protocole DEMP et l'application OASIS, en tant que précurseurs, ont le potentiel de transformer les pratiques actuelles en profondeur. Ce mémoire se veut une première pierre à l'édifice d'une sécurité publique repensée, modernisée et en adéquation avec les aspirations technologiques et sociétales actuelles.

Bibliographie

Are you safe?, *Federal Office for Civil Protection FOCP* [en ligne]. Disponible à l'adresse : https://www.alert.swiss/en/home.html [consulté le 16 août 2024].

asyncio — Asynchronous I/O, *Python documentation* [en ligne]. Disponible à l'adresse : https://docs.python.org/3/library/asyncio.html [consulté le 16 août 2024].

BRAY, Tim, 2017. *The JavaScript Object Notation (JSON) Data Interchange Format*. Internet Engineering Task Force. Request for Comments RFC 8259. DOI 10.17487/RFC8259.

CHF, Chancellerie fédérale. Gestion de crises. [en ligne]. Disponible à l'adresse : https://www.bk.admin.ch/bk/fr/home/dokumentation/fuehrungsunterstuetzung/krisenmanagement.html [consulté le 9 août 2024].

Clients, [en ligne]. Disponible à l'adresse : https://matrix.org/ecosystem/clients/ [consulté le 16 août 2024].

Configuration Manual - Synapse, [en ligne]. Disponible à l'adresse : https://matrix-org.github.io/synapse/latest/usage/configuration/config_documentation.html#ratelimiting [consulté le 16 août 2024].

DU BOYS, Céline et BERTOLUCCI, Marius, 2021. Gouvernance multi-niveaux de la crise de la Covid-19 en France, quels échecs et réussites ? *Gestion et management public*. Vol. 9 / 4, no 4, pp. 49-55. DOI 10.3917/gmp.094.0049.

DUNN, John C., LEWANDOWSKY, Stephan et KIRSNER, Kim, 2002. Dynamics of communication in emergency management. *Applied Cognitive Psychology*. Vol. 16, no 6, pp. 719-737. DOI 10.1002/acp.846.

EchoSOS | Die Notfall-App, 2021 [en ligne]. Disponible à l'adresse : https://echosos.com/ [consulté le 16 août 2024].

ECMA-404, *Ecma International* [en ligne]. Disponible à l'adresse : https://ecma-international.org/publications-and-standards/standards/ecma-404/ [consulté le 10 août 2024].

EL-SAYED, Ammar, ABDELAZIZ, Mahmoud et ABDEL-AZEEM, Mohamed, 2023. Blockchain for Decentralized Emergency Management System. *International Journal of Computing and Digital Systems*. Vol. 14, no 1, pp. 827-837. DOI 10.12785/ijcds/140164.

Extensible Markup Language (XML), [en ligne]. Disponible à l'adresse : https://www.w3.org/XML/ [consulté le 10 août 2024].

FARAZMAND, Ali, 2001. *Handbook of Crisis and Emergency Management*. CRC Press. ISBN 978-1-4200-0245-4. Google-Books-ID: CEpVdPyySp0C

FORD, Kat et al., 2022. The use of mobile phone applications to enhance personal safety from interpersonal violence – an overview of available smartphone applications in the United Kingdom. *BMC Public Health*. Vol. 22, no 1, p. 1158. DOI 10.1186/s12889-022-13551-9.

GnuPG - Validating keys, [en ligne]. Disponible à l'adresse : https://www.gnupg.org/gph/en/manual/x334.html [consulté le 11 août 2024].

HOLZHÜTER, Michael et MEISSEN, Ulrich, 2020. A Decentralized Reference Architecture for Interconnected Systems in Emergency Management. *Emergency Management*.

INITIATIVE (WAI), W3C Web Accessibility. W3C Accessibility Standards Overview. *Web Accessibility Initiative (WAI)* [en ligne]. Disponible à l'adresse : https://www.w3.org/WAI/standards-guidelines/ [consulté le 16 août 2024].

JSON, [en ligne]. Disponible à l'adresse : https://www.json.org/json-en.html [consulté le 10 août 2024].

KAPUCU, Naim et GARAYEV, Vener, 2011. Collaborative Decision-Making in Emergency and Disaster Management. *International Journal of Public Administration*. Vol. 34, no 6, pp. 366-375. DOI 10.1080/01900692.2011.561477.

LIU, Ke, 2023. Discussion on Centralization and Decentralization Patterns in Emergency Management. *Urban Studies and Public Administration*. Vol. 6, no 2, p. p57. DOI 10.22158/uspa.v6n2p57.

Matrix Specification, [en ligne]. Disponible à l'adresse : https://spec.matrix.org/v1.11/ [consulté le 16 août 2024].

matrix-nio/matrix-nio [logiciel] [en ligne]. 15 août 2024. matrix-nio. [consulté le 16 août 2024]. Disponible à l'adresse : https://github.com/matrix-nio/matrix-nio [consulté le 16 août 2024].

MeteoSwiss-App - MeteoSchweiz, [en ligne]. Disponible à l'adresse : https://www.meteoschweiz.admin.ch/service-und-publikationen/service/wetter-und-klimaprodukte/meteoswiss-app.html [consulté le 16 août 2024].

Naming a Package (Java™), [en ligne]. Disponible à l'adresse : https://docs.oracle.com/javase/tutorial/java/package/namingpkgs.html [consulté le 12 août 2024].

nginx, [en ligne]. Disponible à l'adresse : https://nginx.org/en/ [consulté le 16 août 2024].

PANAGIOTOPOULOS, Panos et al., 2016. Social media in emergency management: Twitter as a tool for communicating risks to the public. *Technological Forecasting and Social Change*. Vol. 111, pp. 86-96. DOI 10.1016/j.techfore.2016.06.010.

Premiers secours: une nouvelle application pour mieux réagir, 2023 [en ligne]. Disponible à l'adresse : https://www.redcross.ch/fr/pages-media/premiers-secours-une-nouvelle-application-pour-mieux-reagir [consulté le 16 août 2024].

REGA, Schweizerische Rettungsflugwacht, 2023. Rega-App | Schweizerische Rettungsflugwacht Rega. [en ligne]. 4 septembre 2023. Disponible à l'adresse : https://www.rega.ch/im-einsatz/so-helfen-wir-ihnen/rega-app [consulté le 16 août 2024].

Requests: HTTP for Humans™, [en ligne]. Disponible à l'adresse : https://docs.python-requests.org/en/latest/index.html [consulté le 14 août 2024].

RFC 791 : *Internet Protocol*, 1981. Internet Engineering Task Force. Request for Comments . DOI 10.17487/RFC0791.

RFC 1035 : *Domain names - implementation and specification*, 1987. Internet Engineering Task Force. Request for Comments . DOI 10.17487/RFC1035.

SABRI, Syikh Sazlin Shah et al., 2024. Five Phases Cycles in Emergency Preparedness and Response Plan (EPRP) As An Emergency Management For Campus Environment. *Journal of Advanced Research in Technology and Innovation Management*. Vol. 11, no 1, pp. 12-20.

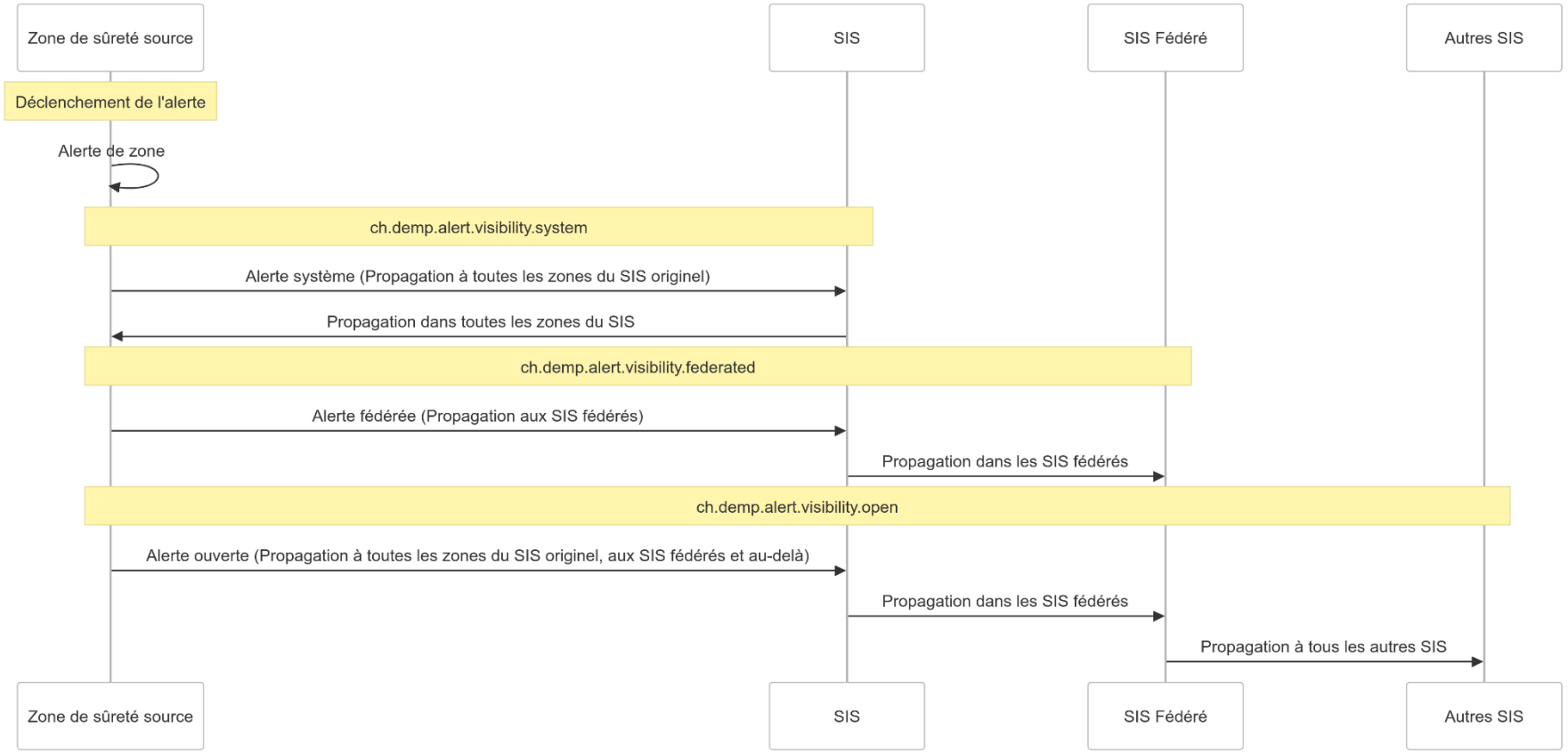
SAINT-ANDRE, Peter, 2011. *Extensible Messaging and Presence Protocol (XMPP): Core*. Internet Engineering Task Force. Request for Comments RFC 6120. DOI 10.17487/RFC6120.

Signal Messenger - Safety Numbers, *Signal Support* [en ligne]. Disponible à l'adresse : https://support.signal.org/hc/en-us/articles/360007060632-What-is-a-safety-number-and-why-do-I-see-that-it-changed [consulté le 11 août 2024].

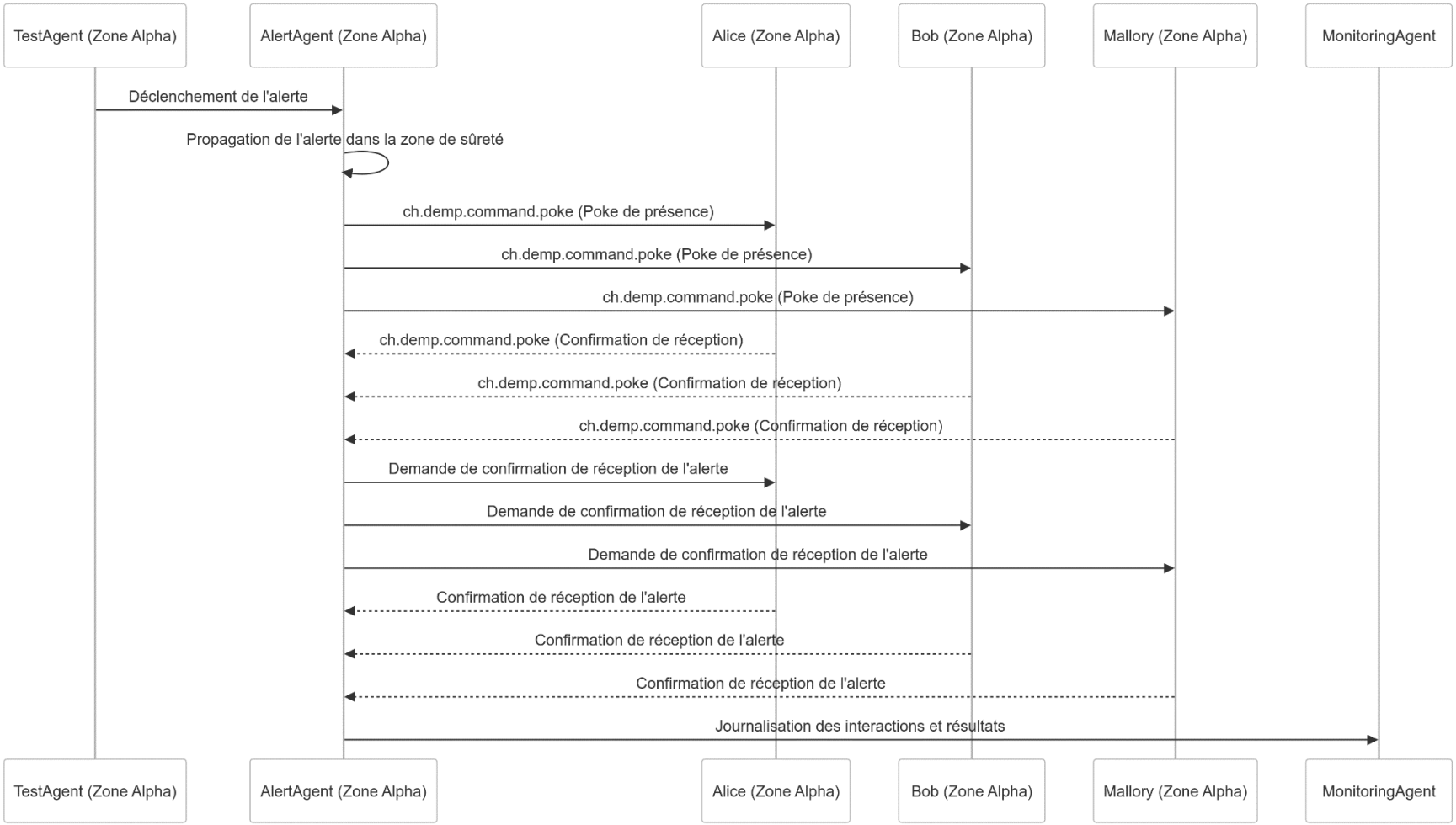
SKAR, Marit, SYDNES, Maria et SYDNES, Are Kristoffer, 2016. Integrating unorganized volunteers in emergency response management: A case study. *International Journal of Emergency Services*. Vol. 5, no 1, pp. 52-65. DOI 10.1108/IJES-04-2015-0017.

SQLite Home Page, [en ligne]. Disponible à l'adresse : https://www.sqlite.org/index.html [consulté le 13 août 2024].

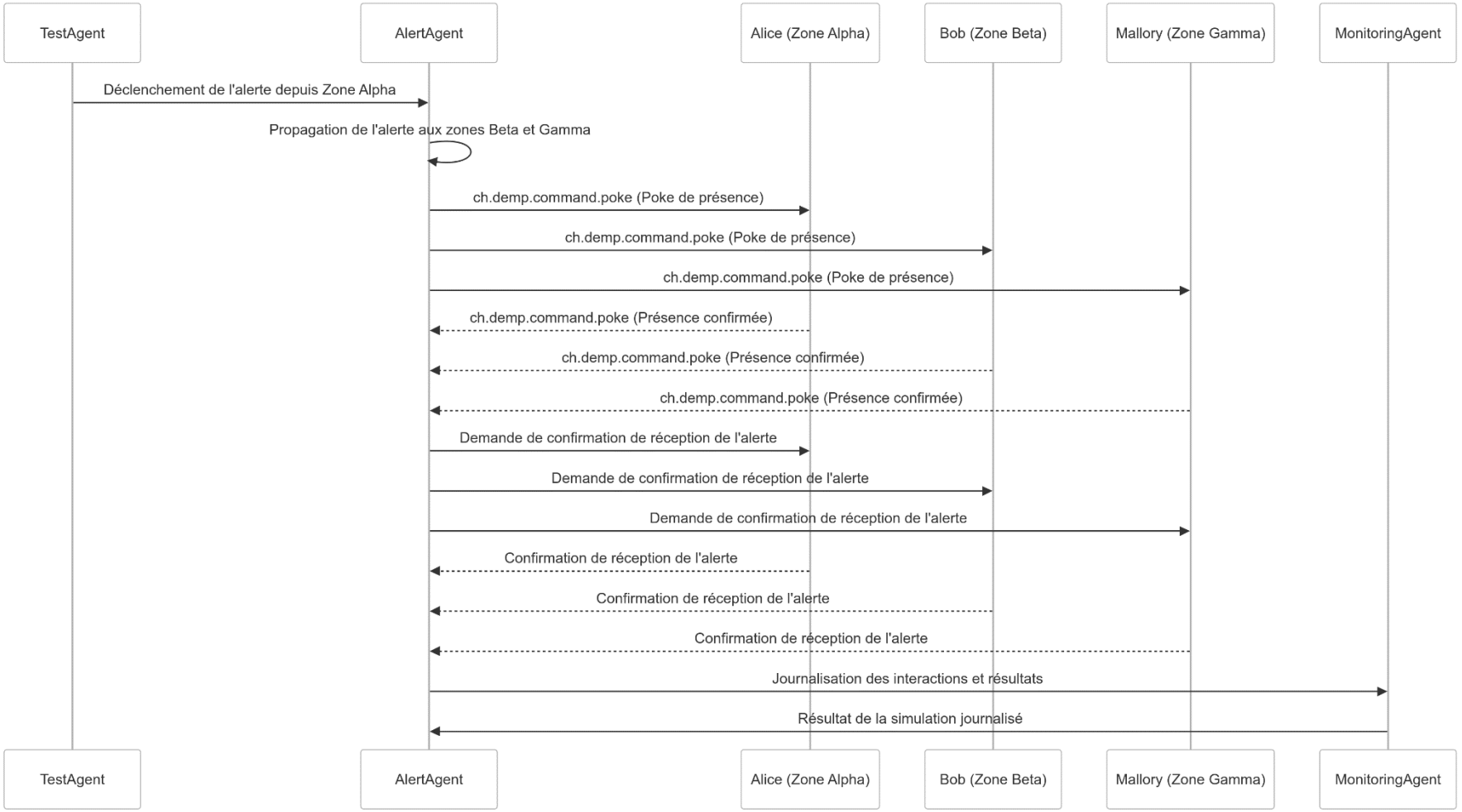
Annexe 1 : Diagramme de séquence de propagation des alertes



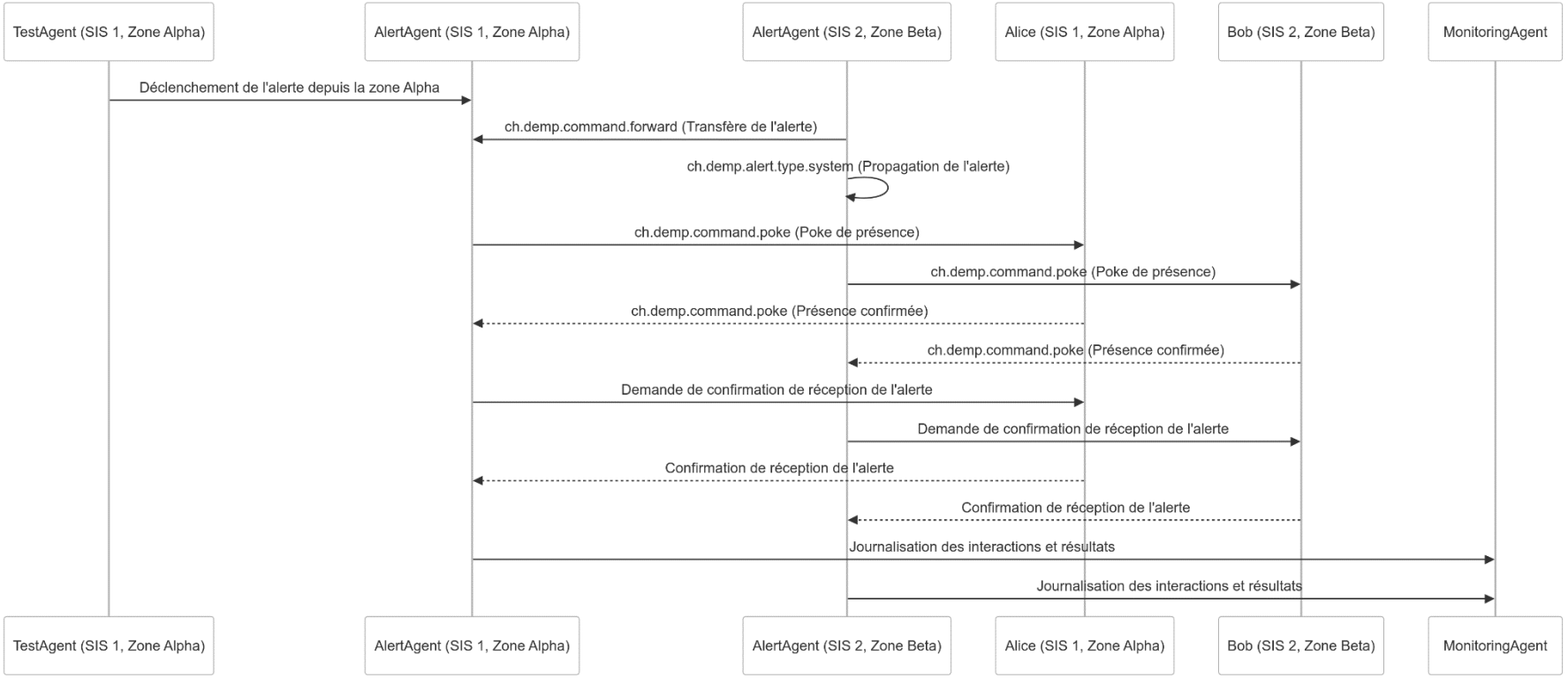
Annexe 2 : Diagramme de séquence Alerte de zone



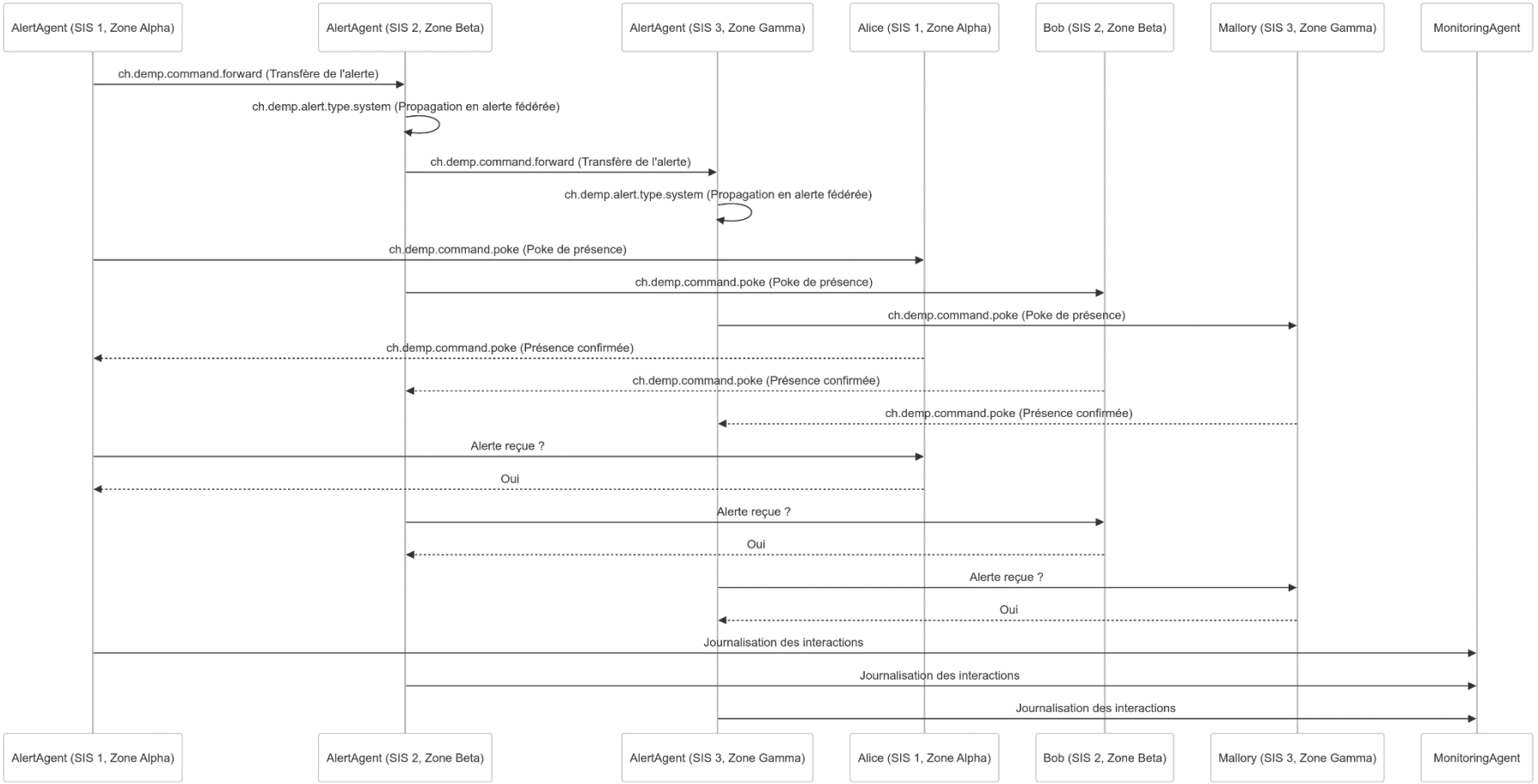
Annexe 3 : Diagramme de séquence Alerte système



Annexe 4 : Diagramme de séquence Alerte fédérée



Annexe 5 : Diagramme de séquence Alerte ouverte



Annexe 6 : Données brutes des simulations

Alerte de Zone 1 :

2024-08-15 15:22:42.250000: @testagent:sis1.oasis.local ch.demp.alert.start !nSlWeddQsbdCiPiCYA:sis1.oasis.local

2024-08-15 15:22:42.497000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !nSlWeddQsbdCiPiCYA:sis1.oasis.local

2024-08-15 15:22:42.538000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alice:sis1.oasis.local !nSlWeddQsbdCiPiCYA:sis1.oasis.local

2024-08-15 15:22:42.575000: @alertagent:sis1.oasis.local ch.demp.sis.poke @bob:sis1.oasis.local !nSlWeddQsbdCiPiCYA:sis1.oasis.local

2024-08-15 15:22:42.624000: @alertagent:sis1.oasis.local ch.demp.sis.poke @mallory:sis1.oasis.local !nSlWeddQsbdCiPiCYA:sis1.oasis.local

2024-08-15 15:22:42.670000: @alice:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !nSlWeddQsbdCiPiCYA:sis1.oasis.local

2024-08-15 15:22:42.712000: @alertagent:sis1.oasis.local ch.demp.sis.poke @monitoringagent:sis1.oasis.local !nSlWeddQsbdCiPiCYA:sis1.oasis.local

2024-08-15 15:22:42.747000: @bob:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !nSlWeddQsbdCiPiCYA:sis1.oasis.local

2024-08-15 15:22:42.807000: @alertagent:sis1.oasis.local ch.demp.sis.poke @testagent:sis1.oasis.local !nSlWeddQsbdCiPiCYA:sis1.oasis.local

2024-08-15 15:22:42.889000: @mallory:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !nSlWeddQsbdCiPiCYA:sis1.oasis.local

Alerte de Zone 2 :

2024-08-15 15:23:30.202000: @testagent:sis1.oasis.local ch.demp.alert.start !sCbekAGOrnHkalwqnf:sis1.oasis.local

2024-08-15 15:23:30.446000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !sCbekAGOrnHkalwqnf:sis1.oasis.local

2024-08-15 15:23:30.480000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alice:sis1.oasis.local !sCbekAGOrnHkalwqnf:sis1.oasis.local

2024-08-15 15:23:30.519000: @alertagent:sis1.oasis.local ch.demp.sis.poke @bob:sis1.oasis.local !sCbekAGOrnHkalwqnf:sis1.oasis.local

2024-08-15 15:23:30.564000: @alertagent:sis1.oasis.local ch.demp.sis.poke @mallory:sis1.oasis.local !sCbekAGOrnHkalwqnf:sis1.oasis.local

2024-08-15 15:23:30.606000: @alice:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !sCbekAGOrnHkalwqnf:sis1.oasis.local

2024-08-15 15:23:30.640000: @alertagent:sis1.oasis.local ch.demp.sis.poke @monitoringagent:sis1.oasis.local !sCbekAGOrnHkalwqnf:sis1.oasis.local

2024-08-15 15:23:30.679000: @bob:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !sCbekAGOrnHkalwqnf:sis1.oasis.local

2024-08-15 15:23:30.721000: @alertagent:sis1.oasis.local ch.demp.sis.poke @testagent:sis1.oasis.local !sCbekAGOrnHkalwqnf:sis1.oasis.local

2024-08-15 15:23:30.756000: @mallory:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !sCbekAGOrnHkalwqnf:sis1.oasis.local

2024-08-15 15:23:30.793000: @alertagent:sis1.oasis.local ch.demp.alert.confirm !sCbekAGOrnHkalwqnf:sis1.oasis.local

Alerte de Zone 3 :

2024-08-15 15:26:33.407000: @testagent:sis1.oasis.local ch.demp.alert.start !FdAwCRBNDDXGKLnfMY:sis1.oasis.local

2024-08-15 15:26:33.655000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !FdAwCRBNDDXGKLnfMY:sis1.oasis.local

2024-08-15 15:26:33.695000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alice:sis1.oasis.local !FdAwCRBNDDXGKLnfMY:sis1.oasis.local

2024-08-15 15:26:33.758000: @alertagent:sis1.oasis.local ch.demp.sis.poke @bob:sis1.oasis.local !FdAwCRBNDDXGKLnfMY:sis1.oasis.local

2024-08-15 15:26:33.815000: @alertagent:sis1.oasis.local ch.demp.sis.poke @mallory:sis1.oasis.local !FdAwCRBNDDXGKLnfMY:sis1.oasis.local

2024-08-15 15:26:34.060000: @mallory:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !FdAwCRBNDDXGKLnfMY:sis1.oasis.local

2024-08-15 15:26:34.084000: @alertagent:sis1.oasis.local ch.demp.alert.confirm !FdAwCRBNDDXGKLnfMY:sis1.oasis.local

2024-08-15 15:26:34.246000: @alice:sis1.oasis.local ch.demp.alert.confirm @alertagent:sis1.oasis.local !FdAwCRBNDDXGKLnfMY:sis1.oasis.local

2024-08-15 15:26:34.282000: @bob:sis1.oasis.local ch.demp.alert.confirm @alertagent:sis1.oasis.local !FdAwCRBNDDXGKLnfMY:sis1.oasis.local

2024-08-15 15:26:34.327000: @mallory:sis1.oasis.local ch.demp.alert.confirm @alertagent:sis1.oasis.local !FdAwCRBNDDXGKLnfMY:sis1.oasis.local

Alerte système 1 :

2024-08-15 15:52:02.391000: @testagent:sis1.oasis.local ch.demp.alert.start !qaxbozWWGsUpkCJVPr:sis1.oasis.local

2024-08-15 15:52:02.604000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !fXDpLsXwVikIPZUtIZ:sis1.oasis.local

2024-08-15 15:52:02.647000: @alertagent:sis1.oasis.local ch.demp.sis.poke @bob:sis1.oasis.local !fXDpLsXwVikIPZUtIZ:sis1.oasis.local

2024-08-15 15:52:02.696000: @alertagent:sis1.oasis.local ch.demp.sis.poke @monitoringagent:sis1.oasis.local !fXDpLsXwVikIPZUtIZ:sis1.oasis.local

2024-08-15 15:52:02.742000: @alertagent:sis1.oasis.local ch.demp.sis.poke @testagent:sis1.oasis.local !fXDpLsXwVikIPZUtIZ:sis1.oasis.local

2024-08-15 15:52:02.759000: @bob:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !fXDpLsXwVikIPZUtIZ:sis1.oasis.local

2024-08-15 15:52:02.803000: @alertagent:sis1.oasis.local ch.demp.alert.confirm !fXDpLsXwVikIPZUtIZ:sis1.oasis.local

2024-08-15 15:52:02.860000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !qaxbozWWGsUpkCJVPr:sis1.oasis.local

2024-08-15 15:52:03.012000: @alertagent:sis1.oasis.local ch.demp.sis.poke @testagent:sis1.oasis.local !qaxbozWWGsUpkCJVPr:sis1.oasis.local

2024-08-15 15:52:03.051000: @alice:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !qaxbozWWGsUpkCJVPr:sis1.oasis.local

2024-08-15 15:52:03.071000: @alertagent:sis1.oasis.local ch.demp.alert.confirm !qaxbozWWGsUpkCJVPr:sis1.oasis.local

2024-08-15 15:52:03.184000: @alice:sis1.oasis.local ch.demp.alert.confirm @alertagent:sis1.oasis.local !qaxbozWWGsUpkCJVPr:sis1.oasis.local

Alerte système 2 :

2024-08-15 15:53:19.174000: @testagent:sis1.oasis.local ch.demp.alert.start !ecGhrPTOWRzUnRyCRh:sis1.oasis.local

2024-08-15 15:53:19.392000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !YHFqeuUIKTtbKQclxj:sis1.oasis.local

2024-08-15 15:53:19.430000: @alertagent:sis1.oasis.local ch.demp.sis.poke @mallory:sis1.oasis.local !YHFqeuUIKTtbKQclxj:sis1.oasis.local

2024-08-15 15:53:19.463000: @alertagent:sis1.oasis.local ch.demp.sis.poke @monitoringagent:sis1.oasis.local !YHFqeuUIKTtbKQclxj:sis1.oasis.local

2024-08-15 15:53:19.518000: @alertagent:sis1.oasis.local ch.demp.alert.confirm !YHFqeuUIKTtbKQclxj:sis1.oasis.local

2024-08-15 15:53:19.529000: @mallory:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !YHFqeuUIKTtbKQclxj:sis1.oasis.local

2024-08-15 15:53:19.585000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !oMGRjsRcPwhURSDRtz:sis1.oasis.local

2024-08-15 15:53:19.688000: @mallory:sis1.oasis.local ch.demp.alert.confirm @alertagent:sis1.oasis.local !YHFqeuUIKTtbKQclxj:sis1.oasis.local

2024-08-15 15:53:19.632000: @alertagent:sis1.oasis.local ch.demp.sis.poke @bob:sis1.oasis.local !oMGRjsRcPwhURSDRtz:sis1.oasis.local

2024-08-15 15:53:19.707000: @alertagent:sis1.oasis.local ch.demp.sis.poke @monitoringagent:sis1.oasis.local !oMGRjsRcPwhURSDRtz:sis1.oasis.local

2024-08-15 15:53:19.769000: @alertagent:sis1.oasis.local ch.demp.sis.poke @testagent:sis1.oasis.local !oMGRjsRcPwhURSDRtz:sis1.oasis.local

2024-08-15 15:53:19.806000: @bob:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !oMGRjsRcPwhURSDRtz:sis1.oasis.local

2024-08-15 15:53:19.868000: @alertagent:sis1.oasis.local ch.demp.alert.confirm !oMGRjsRcPwhURSDRtz:sis1.oasis.local

2024-08-15 15:53:20.072000: @bob:sis1.oasis.local ch.demp.alert.confirm @alertagent:sis1.oasis.local !oMGRjsRcPwhURSDRtz:sis1.oasis.local

2024-08-15 15:53:20.049000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alice:sis1.oasis.local !ecGhrPTOWRzUnRyCRh:sis1.oasis.local

2024-08-15 15:53:20.116000: @alertagent:sis1.oasis.local ch.demp.sis.poke @monitoringagent:sis1.oasis.local !ecGhrPTOWRzUnRyCRh:sis1.oasis.local

2024-08-15 15:53:20.172000: @alertagent:sis1.oasis.local ch.demp.sis.poke @testagent:sis1.oasis.local !ecGhrPTOWRzUnRyCRh:sis1.oasis.local

2024-08-15 15:53:20.210000: @alice:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !ecGhrPTOWRzUnRyCRh:sis1.oasis.local

2024-08-15 15:53:20.242000: @alertagent:sis1.oasis.local ch.demp.alert.confirm !ecGhrPTOWRzUnRyCRh:sis1.oasis.local

2024-08-15 15:53:20.387000: @alice:sis1.oasis.local ch.demp.alert.confirm @alertagent:sis1.oasis.local !ecGhrPTOWRzUnRyCRh:sis1.oasis.local

Alerte système 3 :

2024-08-15 15:54:17.639000: @testagent:sis1.oasis.local ch.demp.alert.start !JPEaekKcyYYeLbSwdS:sis1.oasis.local

2024-08-15 15:54:17.913000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !cvmesSNZWyZGFJfTQq:sis1.oasis.local

2024-08-15 15:54:18.015000: @alertagent:sis1.oasis.local ch.demp.sis.poke @monitoringagent:sis1.oasis.local !cvmesSNZWyZGFJfTQq:sis1.oasis.local

2024-08-15 15:54:18.052000: @alertagent:sis1.oasis.local ch.demp.sis.poke @testagent:sis1.oasis.local !cvmesSNZWyZGFJfTQq:sis1.oasis.local

2024-08-15 15:54:18.098000: @alertagent:sis1.oasis.local ch.demp.alert.confirm !cvmesSNZWyZGFJfTQq:sis1.oasis.local

2024-08-15 15:54:18.176000: @bob:sis1.oasis.local ch.demp.alert.confirm @alertagent:sis1.oasis.local !cvmesSNZWyZGFJfTQq:sis1.oasis.local

Alerte fédérée 1 :

2024-08-15 15:56:01.765000: @testagent:sis1.oasis.local ch.demp.alert.start !HeByRFUzTXHKpUXdiC:sis1.oasis.local

2024-08-15 15:56:02.007000: @alertagent:sis2.oasis.local ch.demp.alert.forward !HeByRFUzTXHKpUXdiC:sis1.oasis.local

2024-08-15 15:56:02.155000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !MjMwEZTVyEzidWytBV:sis2.oasis.local

2024-08-15 15:56:02.051000: @alertagent:sis2.oasis.local ch.demp.alert.start !HeByRFUzTXHKpUXdiC:sis1.oasis.local

2024-08-15 15:56:02.186000: @alertagent:sis2.oasis.local ch.demp.sis.poke @bob:sis2.oasis.local !MjMwEZTVyEzidWytBV:sis2.oasis.local

2024-08-15 15:56:02.218000: @alertagent:sis2.oasis.local ch.demp.sis.poke @monitoringagent:sis2.oasis.local !MjMwEZTVyEzidWytBV:sis2.oasis.local

2024-08-15 15:56:02.261000: @alertagent:sis2.oasis.local ch.demp.alert.confirm !MjMwEZTVyEzidWytBV:sis2.oasis.local

2024-08-15 15:56:02.276000: @bob:sis2.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !MjMwEZTVyEzidWytBV:sis2.oasis.local

2024-08-15 15:56:02.453000: @bob:sis2.oasis.local ch.demp.alert.confirm @alertagent:sis2.oasis.local !MjMwEZTVyEzidWytBV:sis2.oasis.local

2024-08-15 15:56:02.436000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !HeByRFUzTXHKpUXdiC:sis1.oasis.local

2024-08-15 15:56:02.494000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !HeByRFUzTXHKpUXdiC:sis1.oasis.local

2024-08-15 15:56:02.531000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alice:sis1.oasis.local !HeByRFUzTXHKpUXdiC:sis1.oasis.local

2024-08-15 15:56:02.562000: @alertagent:sis2.oasis.local ch.demp.sis.poke @monitoringagent:sis1.oasis.local !HeByRFUzTXHKpUXdiC:sis1.oasis.local

2024-08-15 15:56:02.587000: @alertagent:sis2.oasis.local ch.demp.sis.poke @testagent:sis1.oasis.local !HeByRFUzTXHKpUXdiC:sis1.oasis.local

2024-08-15 15:56:02.769000: @alice:sis1.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !HeByRFUzTXHKpUXdiC:sis1.oasis.local

2024-08-15 15:56:02.613000: @alertagent:sis2.oasis.local ch.demp.alert.confirm !HeByRFUzTXHKpUXdiC:sis1.oasis.local

2024-08-15 15:56:02.910000: @alice:sis1.oasis.local ch.demp.alert.confirm @alertagent:sis2.oasis.local !HeByRFUzTXHKpUXdiC:sis1.oasis.local

Alerte fédérée 2 :

2024-08-15 15:58:04.777000: @testagent:sis1.oasis.local ch.demp.alert.start !bZNBHuWTnAulgYLrPx:sis1.oasis.local

2024-08-15 15:58:05: @alertagent:sis2.oasis.local ch.demp.alert.forward !bZNBHuWTnAulgYLrPx:sis1.oasis.local

2024-08-15 15:58:05.165000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !YGfnpspWGIQcAiolud:sis2.oasis.local

2024-08-15 15:58:05.042000: @alertagent:sis2.oasis.local ch.demp.alert.start !bZNBHuWTnAulgYLrPx:sis1.oasis.local

2024-08-15 15:58:05.196000: @alertagent:sis2.oasis.local ch.demp.sis.poke @bob:sis2.oasis.local !YGfnpspWGIQcAiolud:sis2.oasis.local

2024-08-15 15:58:05.225000: @alertagent:sis2.oasis.local ch.demp.sis.poke @monitoringagent:sis2.oasis.local !YGfnpspWGIQcAiolud:sis2.oasis.local

2024-08-15 15:58:05.272000: @alertagent:sis2.oasis.local ch.demp.alert.confirm !YGfnpspWGIQcAiolud:sis2.oasis.local

2024-08-15 15:58:05.301000: @bob:sis2.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !YGfnpspWGIQcAiolud:sis2.oasis.local

2024-08-15 15:58:05.490000: @bob:sis2.oasis.local ch.demp.alert.confirm @alertagent:sis2.oasis.local !YGfnpspWGIQcAiolud:sis2.oasis.local

2024-08-15 15:58:05.479000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !bZNBHuWTnAulgYLrPx:sis1.oasis.local

2024-08-15 15:58:05.522000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !bZNBHuWTnAulgYLrPx:sis1.oasis.local

2024-08-15 15:58:05.554000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alice:sis1.oasis.local !bZNBHuWTnAulgYLrPx:sis1.oasis.local

2024-08-15 15:58:05.588000: @alertagent:sis2.oasis.local ch.demp.sis.poke @monitoringagent:sis1.oasis.local !bZNBHuWTnAulgYLrPx:sis1.oasis.local

2024-08-15 15:58:05.612000: @alertagent:sis2.oasis.local ch.demp.sis.poke @testagent:sis1.oasis.local !bZNBHuWTnAulgYLrPx:sis1.oasis.local

2024-08-15 15:58:05.799000: @alice:sis1.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !bZNBHuWTnAulgYLrPx:sis1.oasis.local

2024-08-15 15:58:05.638000: @alertagent:sis2.oasis.local ch.demp.alert.confirm !bZNBHuWTnAulgYLrPx:sis1.oasis.local

Alerte fédérée 3 :

2024-08-15 15:59:09.405000: @testagent:sis1.oasis.local ch.demp.alert.start !gtfQURajrjHbohqHya:sis1.oasis.local

2024-08-15 15:59:09.657000: @alertagent:sis2.oasis.local ch.demp.alert.forward !gtfQURajrjHbohqHya:sis1.oasis.local

2024-08-15 15:59:09.681000: @alertagent:sis2.oasis.local ch.demp.alert.start !gtfQURajrjHbohqHya:sis1.oasis.local

2024-08-15 15:59:09.844000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !YrjFMijCSBpkqKugOC:sis2.oasis.local

2024-08-15 15:59:09.872000: @alertagent:sis2.oasis.local ch.demp.sis.poke @bob:sis2.oasis.local !YrjFMijCSBpkqKugOC:sis2.oasis.local

2024-08-15 15:59:09.711000: @alertagent:sis2.oasis.local ch.demp.alert.forward !gtfQURajrjHbohqHya:sis1.oasis.local

2024-08-15 15:59:09.905000: @alertagent:sis2.oasis.local ch.demp.sis.poke @monitoringagent:sis2.oasis.local !YrjFMijCSBpkqKugOC:sis2.oasis.local

2024-08-15 15:59:09.732000: @alertagent:sis2.oasis.local ch.demp.alert.start !gtfQURajrjHbohqHya:sis1.oasis.local

Alerte ouverte 1 :

2024-08-15 16:11:19.039000: @testagent:sis1.oasis.local ch.demp.alert.start !FTHOEJHhHXyRcDMaQW:sis1.oasis.local

2024-08-15 16:11:19.404000: @alertagent:sis1.oasis.local ch.demp.alert.forward !FTHOEJHhHXyRcDMaQW:sis1.oasis.local

2024-08-15 16:11:19.506000: @alertagent:sis1.oasis.local ch.demp.alert.start !FTHOEJHhHXyRcDMaQW:sis1.oasis.local

2024-08-15 16:11:19.675000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !FTHOEJHhHXyRcDMaQW:sis1.oasis.local

2024-08-15 16:11:19.793000: @alertagent:sis2.oasis.local ch.demp.alert.forward !EIRSBteztyKUvXNeCN:sis2.oasis.local

2024-08-15 16:11:19.817000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !FTHOEJHhHXyRcDMaQW:sis1.oasis.local

2024-08-15 16:11:20.070000: @alertagent:sis1.oasis.local ch.demp.sis.poke @monitoringagent:sis1.oasis.local !FTHOEJHhHXyRcDMaQW:sis1.oasis.local

2024-08-15 16:11:20.158000: @alertagent:sis1.oasis.local ch.demp.sis.poke @testagent:sis1.oasis.local !FTHOEJHhHXyRcDMaQW:sis1.oasis.local

2024-08-15 16:11:20.226000: @alertagent:sis1.oasis.local ch.demp.alert.confirm !FTHOEJHhHXyRcDMaQW:sis1.oasis.local

2024-08-15 16:11:20.462000: @alice:sis1.oasis.local ch.demp.alert.confirm @alertagent:sis1.oasis.local !FTHOEJHhHXyRcDMaQW:sis1.oasis.local

2024-08-15 16:11:20.180000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !EIRSBteztyKUvXNeCN:sis2.oasis.local

2024-08-15 16:11:20.397000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alertagent:sis3.oasis.local !EIRSBteztyKUvXNeCN:sis2.oasis.local

2024-08-15 16:11:20.577000: @alertagent:sis2.oasis.local ch.demp.sis.poke @bob:sis2.oasis.local !EIRSBteztyKUvXNeCN:sis2.oasis.local

2024-08-15 16:11:21.017000: @bob:sis2.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !EIRSBteztyKUvXNeCN:sis2.oasis.local

Alerte ouverte 2 :

2024-08-15 16:14:22.152000: @testagent:sis1.oasis.local ch.demp.alert.start !vrAXeYMxLYPxYrbzvc:sis1.oasis.local

2024-08-15 16:14:22.673000: @alertagent:sis1.oasis.local ch.demp.alert.forward !vrAXeYMxLYPxYrbzvc:sis1.oasis.local

2024-08-15 16:14:22.793000: @alertagent:sis1.oasis.local ch.demp.alert.start !vrAXeYMxLYPxYrbzvc:sis1.oasis.local

2024-08-15 16:14:23.004000: @alertagent:sis2.oasis.local ch.demp.alert.forward !dufxrjypRkKWJonNLg:sis2.oasis.local

2024-08-15 16:14:23.032000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !vrAXeYMxLYPxYrbzvc:sis1.oasis.local

2024-08-15 16:14:23.129000: @alertagent:sis2.oasis.local ch.demp.alert.start !dufxrjypRkKWJonNLg:sis2.oasis.local

2024-08-15 16:14:23.265000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !vrAXeYMxLYPxYrbzvc:sis1.oasis.local

2024-08-15 16:14:23.391000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alice:sis1.oasis.local !vrAXeYMxLYPxYrbzvc:sis1.oasis.local

2024-08-15 16:14:23.012000: @alertagent:sis3.oasis.local ch.demp.alert.forward !dufxrjypRkKWJonNLg:sis2.oasis.local

2024-08-15 16:14:23.510000: @alertagent:sis1.oasis.local ch.demp.sis.poke @monitoringagent:sis1.oasis.local !vrAXeYMxLYPxYrbzvc:sis1.oasis.local

2024-08-15 16:14:23.431000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !dufxrjypRkKWJonNLg:sis2.oasis.local

2024-08-15 16:14:23.077000: @alertagent:sis3.oasis.local ch.demp.alert.start !dufxrjypRkKWJonNLg:sis2.oasis.local

2024-08-15 16:14:23.642000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alertagent:sis3.oasis.local !dufxrjypRkKWJonNLg:sis2.oasis.local

2024-08-15 16:14:23.862000: @alertagent:sis3.oasis.local ch.demp.sis.poke @alertagent:sis3.oasis.local !ncvxWFBoLgZuhdjQBH:sis3.oasis.local

2024-08-15 16:14:23.675000: @alertagent:sis1.oasis.local ch.demp.sis.poke @testagent:sis1.oasis.local !vrAXeYMxLYPxYrbzvc:sis1.oasis.local

2024-08-15 16:14:24.072000: @alertagent:sis3.oasis.local ch.demp.sis.poke @monitoringagent:sis3.oasis.local !ncvxWFBoLgZuhdjQBH:sis3.oasis.local

2024-08-15 16:14:24.198000: @alertagent:sis3.oasis.local ch.demp.alert.confirm !ncvxWFBoLgZuhdjQBH:sis3.oasis.local

2024-08-15 16:14:24.098000: @alertagent:sis2.oasis.local ch.demp.sis.poke @monitoringagent:sis2.oasis.local !dufxrjypRkKWJonNLg:sis2.oasis.local

2024-08-15 16:14:24.418000: @mallory:sis3.oasis.local ch.demp.alert.confirm @alertagent:sis3.oasis.local !ncvxWFBoLgZuhdjQBH:sis3.oasis.local

2024-08-15 16:14:24.323000: @alertagent:sis2.oasis.local ch.demp.alert.confirm !dufxrjypRkKWJonNLg:sis2.oasis.local

2024-08-15 16:14:25.082000: @bob:sis2.oasis.local ch.demp.alert.confirm @alertagent:sis2.oasis.local !dufxrjypRkKWJonNLg:sis2.oasis.local

Alerte ouverte 3 :

2024-08-15 16:18:59.025000: @testagent:sis1.oasis.local ch.demp.alert.start !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.148000: @alertagent:sis1.oasis.local ch.demp.alert.forward !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.184000: @alertagent:sis1.oasis.local ch.demp.alert.start !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.224000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.254000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.312000: @alertagent:sis2.oasis.local ch.demp.alert.forward !hkRcFTsjfTpbPMrfFF:sis2.oasis.local

2024-08-15 16:18:59.303000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alice:sis1.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.361000: @alertagent:sis2.oasis.local ch.demp.alert.start !hkRcFTsjfTpbPMrfFF:sis2.oasis.local

2024-08-15 16:18:59.386000: @alertagent:sis1.oasis.local ch.demp.sis.poke @monitoringagent:sis1.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.454000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !hkRcFTsjfTpbPMrfFF:sis2.oasis.local

2024-08-15 16:18:59.448000: @alertagent:sis1.oasis.local ch.demp.sis.poke @testagent:sis1.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.481000: @alice:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.352000: @alertagent:sis3.oasis.local ch.demp.alert.forward !hkRcFTsjfTpbPMrfFF:sis2.oasis.local

2024-08-15 16:18:59.519000: @alertagent:sis1.oasis.local ch.demp.alert.confirm !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.523000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alertagent:sis3.oasis.local !hkRcFTsjfTpbPMrfFF:sis2.oasis.local

2024-08-15 16:18:59.379000: @alertagent:sis3.oasis.local ch.demp.alert.start !hkRcFTsjfTpbPMrfFF:sis2.oasis.local

2024-08-15 16:18:59.604000: @alertagent:sis2.oasis.local ch.demp.sis.poke @bob:sis2.oasis.local !hkRcFTsjfTpbPMrfFF:sis2.oasis.local

2024-08-15 16:18:59.698000: @alertagent:sis3.oasis.local ch.demp.sis.poke @alertagent:sis3.oasis.local !eASUbCibYkBMMtAGBw:sis3.oasis.local

2024-08-15 16:18:59.638000: @alertagent:sis1.oasis.local ch.demp.alert.forward !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.670000: @alice:sis1.oasis.local ch.demp.alert.confirm @alertagent:sis1.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.697000: @alertagent:sis1.oasis.local ch.demp.alert.start !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.737000: @alertagent:sis3.oasis.local ch.demp.sis.poke @mallory:sis3.oasis.local !eASUbCibYkBMMtAGBw:sis3.oasis.local

2024-08-15 16:18:59.434000: @alertagent:sis3.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !hkRcFTsjfTpbPMrfFF:sis2.oasis.local

2024-08-15 16:18:59.781000: @alertagent:sis3.oasis.local ch.demp.sis.poke @monitoringagent:sis3.oasis.local !eASUbCibYkBMMtAGBw:sis3.oasis.local

2024-08-15 16:18:59.791000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.691000: @alertagent:sis2.oasis.local ch.demp.sis.poke @monitoringagent:sis2.oasis.local !hkRcFTsjfTpbPMrfFF:sis2.oasis.local

2024-08-15 16:18:59.824000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.871000: @alertagent:sis1.oasis.local ch.demp.sis.poke @alice:sis1.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.457000: @alertagent:sis3.oasis.local ch.demp.sis.poke @alertagent:sis3.oasis.local !hkRcFTsjfTpbPMrfFF:sis2.oasis.local

2024-08-15 16:18:59.799000: @alertagent:sis2.oasis.local ch.demp.alert.confirm !hkRcFTsjfTpbPMrfFF:sis2.oasis.local

2024-08-15 16:18:59.830000: @alertagent:sis3.oasis.local ch.demp.alert.confirm !eASUbCibYkBMMtAGBw:sis3.oasis.local

2024-08-15 16:18:59.910000: @alertagent:sis1.oasis.local ch.demp.sis.poke @monitoringagent:sis1.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:18:59.853000: @mallory:sis3.oasis.local ch.demp.sis.poke @alertagent:sis3.oasis.local !eASUbCibYkBMMtAGBw:sis3.oasis.local

2024-08-15 16:18:59.836000: @bob:sis2.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !hkRcFTsjfTpbPMrfFF:sis2.oasis.local

2024-08-15 16:18:59.939000: @alice:sis1.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:19:00.028000: @mallory:sis3.oasis.local ch.demp.alert.confirm @alertagent:sis3.oasis.local !eASUbCibYkBMMtAGBw:sis3.oasis.local

2024-08-15 16:19:00.019000: @alertagent:sis1.oasis.local ch.demp.alert.confirm !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:19:00.071000: @bob:sis2.oasis.local ch.demp.alert.confirm @alertagent:sis2.oasis.local !hkRcFTsjfTpbPMrfFF:sis2.oasis.local

2024-08-15 16:19:00.134000: @alice:sis1.oasis.local ch.demp.alert.confirm @alertagent:sis1.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:19:00.095000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alertagent:sis1.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:19:00.164000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:19:00.253000: @alertagent:sis2.oasis.local ch.demp.sis.poke @alice:sis1.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:19:00.307000: @alertagent:sis2.oasis.local ch.demp.sis.poke @monitoringagent:sis1.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:19:00.416000: @alice:sis1.oasis.local ch.demp.sis.poke @alertagent:sis2.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:19:00.345000: @alertagent:sis2.oasis.local ch.demp.sis.poke @testagent:sis1.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:19:00.375000: @alertagent:sis2.oasis.local ch.demp.alert.confirm !JPHCDLeiyeESVJlgqe:sis1.oasis.local

2024-08-15 16:19:00.563000: @alice:sis1.oasis.local ch.demp.alert.confirm @alertagent:sis2.oasis.local !JPHCDLeiyeESVJlgqe:sis1.oasis.local