**NIS (Network Information Service)**

**Présentation :**

**Network Information Service** (NIS) initialement connu sous le nom de **Yellow Pages** (le nom a été changé en raison du dépôt de la marque par une autre entreprise [British Telecom], elle a été renommée NIS), est un protocole client-serveur développé par Sun Microsystems dans les années 1980, permettant la mise en place d’un système d’annuaire centralisé pour les réseaux UNIX.

N. B. : Les commandes NIS commencent toutes par **yp** (yellow pages)

Exemples de quelques commandes NIS :

**ypbind :** Démarre le service NIS client qui lie la machine à un serveur NIS.

**ypwhich :** Affiche le serveur NIS auquel le client est lié.

**ypcat :** Affiche le contenu des maps NIS

**ypmatch :** Recherche des entrées spécifiques dans les maps NIS

**ypserv :** Démarre le service NIS serveur.

**Fonctionnement :**

Le **serveur NIS** centralise et stocke les informations de configuration telles que les fichiers de mots de passe (/etc/passwd), les fichiers de groupe (/etc/group), les noms d’hôtes (/etc/hosts),etc. dans des bases de données (Maps).

Le **client NIS** interroge le serveur via le protocole RPC, afin d’accéder à la base de données et de récupérer les informations nécessaires à l’authentification d’un utilisateur.

En clair, lorsque l’utilisateur souhaite se connecter, le client NIS envoie une requête au serveur NIS pour récupérer les informations nécessaires à l’authentification.

**Avantages :**

NIS est simple à configurer et à utiliser dans les environnements UNIX et Linux.

Il permet notamment de centraliser les comptes utilisateurs et les informations de configuration, ce qui facilite la gestion de ces données.

**Inconvénients :**

NIS est réputé pour ses faiblesses en matière de sécurité, puisqu’il transmet des données non chiffrées. Les informations telles que les mots de passe peuvent être facilement interceptées si elles ne sont pas bien protégées. Ainsi, les mots de passe peuvent être facilement compromis.

Malheureusement, NIS est de moins en moins adapté aux environnements modernes dû à sa difficulté à évoluer dans les grandes infrastructures, puisqu'il n'est pas conçu pour gérer des milliers de clients efficacement, contrairement à d’autres solutions comme LDAP.

Étant de plus en plus abandonné, il y a de moins en moins de supports et de mises à jour comparé à ses concurrents les plus modernes.

**CAS (Central Authentication Service)**

**Présentation :**

**Central Authentication Service** (CAS) est un système d’authentification unique (SSO - Single Sign-On) pour les applications web développé par **Shawn Bayern**, un chercheur de l’université de Yale au début des années 2000. Il est aujourd’hui utilisé par plusieurs universités (par exemple l’Université Sorbonne Paris Nord) et entreprises dans le monde.

**Fonctionnement :**

Le système CAS est essentiellement basé sur des requêtes HTTP permettant aux utilisateurs de se connecter en une seule fois pour accéder à plusieurs services web. Cela évite à l’utilisateur de s’authentifier à chaque fois qu’il accède à une application grâce à la mise en place d’un système de ticket qui vérifie l’identité de l’utilisateur sans transmettre les informations d’identification (par exemple les mots de passe).

En résumé, lorsque l’utilisateur se connecte à un service sur une page de connexion centralisée, le CAS vérifie les informations d’identification et crée une session unique partagée entre les différents services.

Principe des tickets :

Si l'authentification est réussie, le CAS génère un Ticket de Service (ST) et redirige l’utilisateur vers l’application sur laquelle il s’est connecté avec le ticket qui a été généré.

Le ticket de service sert à authentifier l’utilisateur pour une application ; il peut être utilisé qu’une seule et unique fois, étant donné qu’il est spécifique à une application.

Suite à la première authentification, le CAS génère un Ticket-Granting Cookie (TGC - un cookie de session) qui sera stocké dans un cookie sécurisé dans le navigateur de l’utilisateur. Ce ticket permet également de générer de nouveaux tickets de service (ST) permettant l’accès à d'autres applications sans redemander les informations d’identification.

**Avantages :**

Le système CAS utilise le protocole HTTPS pour transmettre des données d’authentification ce qui les protège contre les interceptions et réduit le risque d’être compromis.

Les tickets générés sont uniques et expirent après une certaine période, ce qui réduit l’utilisation abusive.

Les utilisations ont la possibilité de se connecter une seule fois pour accéder à plusieurs services sans devoir se reconnecter, ce qui améliore l’expérience utilisateur.

CAS peut également supporter d’autres mécanismes d’authentification unique (OAuth, OpenID, SAML).

Lorsqu’un utilisateur se déconnecte, toutes les sessions sont également déconnectées, ce qui améliore grandement la sécurité.

**Inconvénients :**

La mise en place et la configuration de ce système peuvent être complexes en raison du manque de compétences et de la mauvaise compréhension des protocoles d’authentification.

Dans le cas où le serveur CAS est indisponible, il est impossible pour les utilisateurs de s’authentifier, ce qui entraîne une interruption totale des services.

Ce système peut perdre de la performance si le nombre de requêtes d’authentification est très élevé.

Il n'est pas compatible avec certaines applications, ce qui peut limiter son utilisation dans certains environnements.

**Comparaison entre NIS et CAS**

**Sécurité :**

* NIS : Ce mécanisme est plutôt faible en terme de sécurité, car les données transmises ne sont pas chiffrées, ce qui les rend vulnérables aux interceptions
* CAS : Ce système propose une haute sécurité grâce à l’utilisation du protocole HTTPS. L’utilisation de tickets temporaires et uniques pour l’authentification réduit les usages abusifs des données d’authentification

**Expérience utilisateur :**

* NIS : Chaque application nécessite une authentification, obligeant donc l’utilisateur à se connecter plusieurs fois.
* CAS : Le CAS améliore le confort utilisateur en permettant une authentification unique (SSO). Lorsque l’utilisateur est authentifié, il est possible pour lui d’accéder à plusieurs applications sans devoir se reconnecter, ce qui simplifie l’expérience.

**Flexibilité :**

* NIS : NIS est moins flexible et moins adapté à des environnements comptant de nombreux utilisateurs ou des infrastructures complexes (ex : en entreprise). Il sera également amené à rencontrer des difficultés d’évolution pour répondre aux besoins.
* CAS : Contrairement à NIS, il est très flexible puisqu’il peut être adapté à des environnements modernes et complexes. Nous pouvons l’intégrer avec plusieurs systèmes d’authentification et a la possibilité d’évoluer pour répondre aux besoins qui pourraient se faire.

**Développement :**

* NIS : La mise en place de ce système est plutôt simple dans les environnements UNIX. Il est facile à configurer et à utiliser pour les petites infrastructures.
* CAS : La mise en place de CAS est complexe puisqu’elle nécessite des connaissances techniques spécifiques et une bonne compréhension des protocoles utilisés pour l’authentification.

**Conclusion :**

En résumé, NIS est une solution simple et centralisée pour les petits environnements. Cependant, elle est très limitée en termes de sécurité et de flexibilité. En revanche, le système CAS est une solution d’authentification unique sécurisée et très flexible, pouvant être adaptée à différents environnements modernes et complexes, malgré une mise en œuvre complexe qui est strictement nécessaire afin de garantir son bon fonctionnement ainsi qu’une sécurité infaillible.

**Bibliographie**

**NIS :**

IBM “Network Information Service” (page consultée le 17 mai 2024), adresse URL :

[Network Information Service](https://www.ibm.com/docs/fr/aix/7.3?topic=nis-network-information-service)

Wikipédia “Network Information Service” (page consultée le 17 mai 2024), adresse URL :

[Network Information Service — Wikipédia](https://fr.wikipedia.org/wiki/Network_Information_Service)

Oracle “About NIS Authentication” (page consultée le 17 mai 2024), adresse URL :

[3.4.4 About NIS Authentication](https://docs.oracle.com/en/operating-systems/oracle-linux/6/security/ol_nisauth_sec.html)

ggn.dronacharya.info “The Network Information System” (page consultée le 17 mai 2024), adresse URL :

[The Network Information System](https://ggn.dronacharya.info/ITDept/Downloads/QuestionBank/Odd/VIIsem/S&NA/Section-D/S&NA_4.pdf)

Linux Portal “NIS” (page consultée le 17 mai 2024), adresse URL :

[NIS (Network Information Service) | Linux portal](https://en.linuxportal.info/encyclopedia/n/nis-network-information-service-encyclopedia)

**CAS :**

Wikipédia “Central Authentication Service” (page consultée le 17 mai 2024), adresse URL :

[Central Authentication Service — Wikipédia](https://fr.wikipedia.org/wiki/Central_Authentication_Service)

Okta “Qu’est-ce que le protocole CAS ?” (page consultée le 17 mai 2024), adresse URL :

[Qu’est-ce que le protocole CAS (Central Authentication Service) ? | Okta](https://www.okta.com/fr/identity-101/central-authentication-service/)

Wikipédia “Shawn Bayern” (page consultée le 17 mai 2024), adresse URL :

[Shawn Bayern - Wikipedia](https://en.wikipedia.org/wiki/Shawn_Bayern)

Guide Open Source “CAS / Authentification, fédération et de gestion d’identité” (page consultée le 17 mai 2024), adresse URL :

[CAS / Authentification, fédération et de gestion d’identité / Guide Open Source](https://open-source-guide.com/Solutions/Developpement-et-couches-intermediaires/Authentification-federation-et-de-gestion-d-identite/Cas#:~:text=Central%20Authentication%20Service%20est%20un,%C3%A0%20l'universit%C3%A9%20de%20Yale).

ESUP “Présentation de CAS” (page consultée le 17 mai 2024), adresse URL :

[ESUP-Portail - Présentation de CAS (Central Authentication Service)](https://www.esup-portail.org/consortium/espace/SSO_1B/cas/)

Bravas “Avantages et inconvénients de l'authentification unique (SSO) pour les PME ” (page consultée le 17 mai 2024), adresse URL :

[Avantages et inconvénients de l'authentification unique (SSO) pour les PME](https://www.bravas.io/blog-post/avantages-et-inconvenients-de-lauthentification-unique-sso-pour-les-pme)

Geekflare “Qu'est-ce que l'authentification unique et comment fonctionne-t-elle ? Avantages et inconvénients ” (page consultée le 17 mai 2024), adresse URL :

[Qu'est-ce que l'authentification unique et comment fonctionne-t-elle ? Avantages et inconvénients](https://geekflare.com/fr/single-sign-on-work-benefits-drawbacks/)