Découvrir ServiceNow ITSM avec une instance développeur et un MID Server

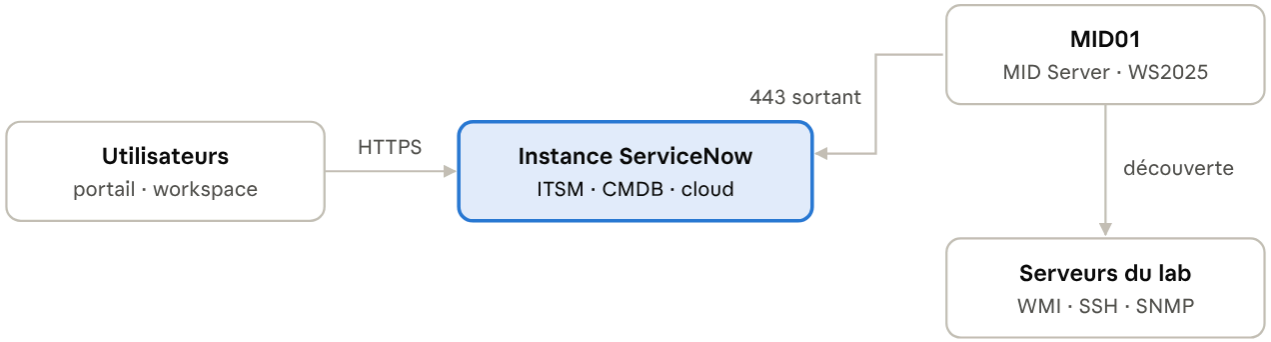
Nov 27, 2026 · @Serge Martins

Objectif

Obtenir une **instance développeur personnelle (PDI)** ServiceNow gratuite, y pratiquer les processus ITSM (incidents, demandes, problèmes, changements, CMDB), puis relier l'instance au réseau **martinscie.lan** grâce à un **MID Server** installé sur Windows Server 2025, pour découvrir automatiquement les serveurs du lab.

Élément	Valeur
Plateforme	ServiceNow AI Platform, version « Australia » (ou « Brazil » selon la date de création de l'instance)
Instance	PDI gratuite, https://devXXXXX.service-now.com
MID Server	MID01 · 192.168.10.49 · Windows Server 2025, membre de martinscie.lan
Accès réseau	Sortant uniquement : HTTPS 443 de MID01 vers l'instance
Prérequis	Compte sur developer.servicenow.com, navigateur récent

Le MID Server relie le lab à l'instance ServiceNow sans port entrant



ServiceNow · instance cloud et MID Server du lab

L'instance est hébergée dans le cloud de ServiceNow ; MID01 s'y connecte en sortie et interroge pour elle les serveurs internes, dont les résultats remplissent la CMDB.

Étape 1 – Obtenir une instance développeur

1. Créer un compte gratuit sur **developer.servicenow.com**.
2. **Request Instance** : choisir la dernière version proposée ; l'instance est prête en quelques minutes.
3. Noter l'URL et le mot de passe `admin` fournis.
4. L'instance se met en veille après une période d'inactivité et est récupérée si elle n'est plus utilisée : y revenir régulièrement et sauvegarder son travail (Update Sets).

Étape 2 – Prendre en main l'interface

- **Navigateur d'applications** (« All ») : rechercher *Incident*, *Problem*, *Change*, *Service Catalog*, *CMDB*.
- **Service Operations Workspace** : espace de travail moderne de l'agent de support.
- **Portail en libre-service** : `https://devXXXXX.service-now.com/sp` côté utilisateur.
- Rôles : `itil` pour les techniciens, `admin` pour l'administration, utilisateur sans rôle pour les demandeurs.

Étape 3 – Configurer l'organisation martinscie

1. **Organization → Companies** : créer « Martins & Cie ».
2. **User Administration → Groups** : groupes d'affectation `Support N1`, `Support N2`, `Réseau`.
3. **Users** : créer quelques utilisateurs (techniciens avec le rôle `itil`, demandeurs sans rôle). En production, ils seraient importés depuis l'AD par LDAP ou par synchronisation Entra ID.
4. **Assignment rules** : affecter automatiquement les incidents de catégorie *Network* au groupe Réseau.

Étape 4 – Pratiquer l'ITSM

Processus	Exercice
Incident	Un demandeur signale « Imprimante injoignable » depuis le portail ; le technicien N1 qualifie (impact, urgence → priorité), escalade en N2, résout et clôture

Processus	Exercice
Demande (catalogue)	Créer un article « Demande de compte AD » avec variables (nom, service) et un flux d'approbation par le manager dans Flow Designer
Problème	Regrouper plusieurs incidents identiques, documenter la cause racine et la solution de contournement
Changement	Changement normal « Mise à jour de pfSense » avec évaluation des risques, approbation CAB et plan de retour arrière
Base de connaissances	Publier un article « Réinitialiser son mot de passe »
SLA	Définir un SLA de résolution P1 en 4 h et observer le suivi

Étape 5 – Installer un MID Server sur MID01

Le **MID Server** est un service Java installé dans le réseau interne : il ouvre une connexion **sortante** HTTPS vers l'instance et exécute pour elle la découverte et les intégrations, sans ouvrir de port entrant.

1. Dans l'instance : **MID Server → Downloads** → télécharger l'installeur Windows 64 bits.
2. Créer un utilisateur `mid.user` avec le rôle `mid_server`.
3. Sur MID01 (Windows Server 2025 joint au domaine) : lancer l'installeur, indiquer l'URL de l'instance, `mid.user` et son mot de passe, le nom `MID01-LAB`, et un compte de service.
4. Dans l'instance : **MID Server → Servers** → `MID01-LAB` doit apparaître **Up** ; cliquer **Validate**.
5. Autoriser sur RFW01 le flux sortant de MID01 vers Internet en 443.

Étape 6 – Découverte de martinscie.lan

1. **Discovery → Credentials** : identifiants Windows (compte de service du domaine avec droits WMI), SSH (compte Linux dédié par clé) et SNMP (communauté en lecture seule).
2. **Discovery → Discovery Schedules → New** : type *Configuration items*, MID Server `MID01-LAB`, plage 192.168.10.0/24.

3. Lancer **Discover now**, suivre le statut, puis consulter **CMDB → Servers** : DC01, PARC01, MAIL01… apparaissent avec leurs logiciels et relations.

> Selon les droits de l'instance développeur, certaines fonctions de Discovery peuvent nécessiter l'activation d'un plugin depuis le portail développeur.

Sécurité et bonnes pratiques

- Ne jamais mettre de données réelles ou personnelles dans une instance développeur.
- Comptes de découverte à privilèges limités ; mot de passe fort pour `admin` et `mid.user`.
- Maintenir le MID Server à jour (il se met à niveau automatiquement avec l'instance).
- Exporter ses développements en Update Sets.

Dépannage

Symptôme	Piste
MID Server « Down »	Flux 443 sortant bloqué, proxy, mot de passe de `mid.user`
Découverte sans résultat	Identifiants refusés, WMI/SSH filtré par le pare-feu, mauvaise plage IP
Instance indisponible	Instance en veille : la réveiller depuis le portail développeur