Présentation NAC

Opérations mondiales de l'infrastructure et des systèmes • Services aux utilisateurs finaux et à l'infrastructure • **Services à la clientèle**

Version 1.1 • 10.01.2025

faurecia
inspiring mobility

Contenu

Introduction

Ce document définis ce qu'est le contrôle d'accès réseaux

Contrôle d'accès réseau (NAC)

Le contrôle d'accès au réseau (NAC), également connu sous le nom de contrôle d'admission au réseau, est le processus consistant à empêcher les utilisateurs et appareils non autorisés d'accéder à un réseau d'entreprise ou privé. Le NAC garantit que seuls les utilisateurs authentifiés et les dispositifs autorisés et conformes aux politiques de sécurité peuvent pénétrer dans le réseau.

1. Pourquoi Faurecia a besoin de le mettre en place

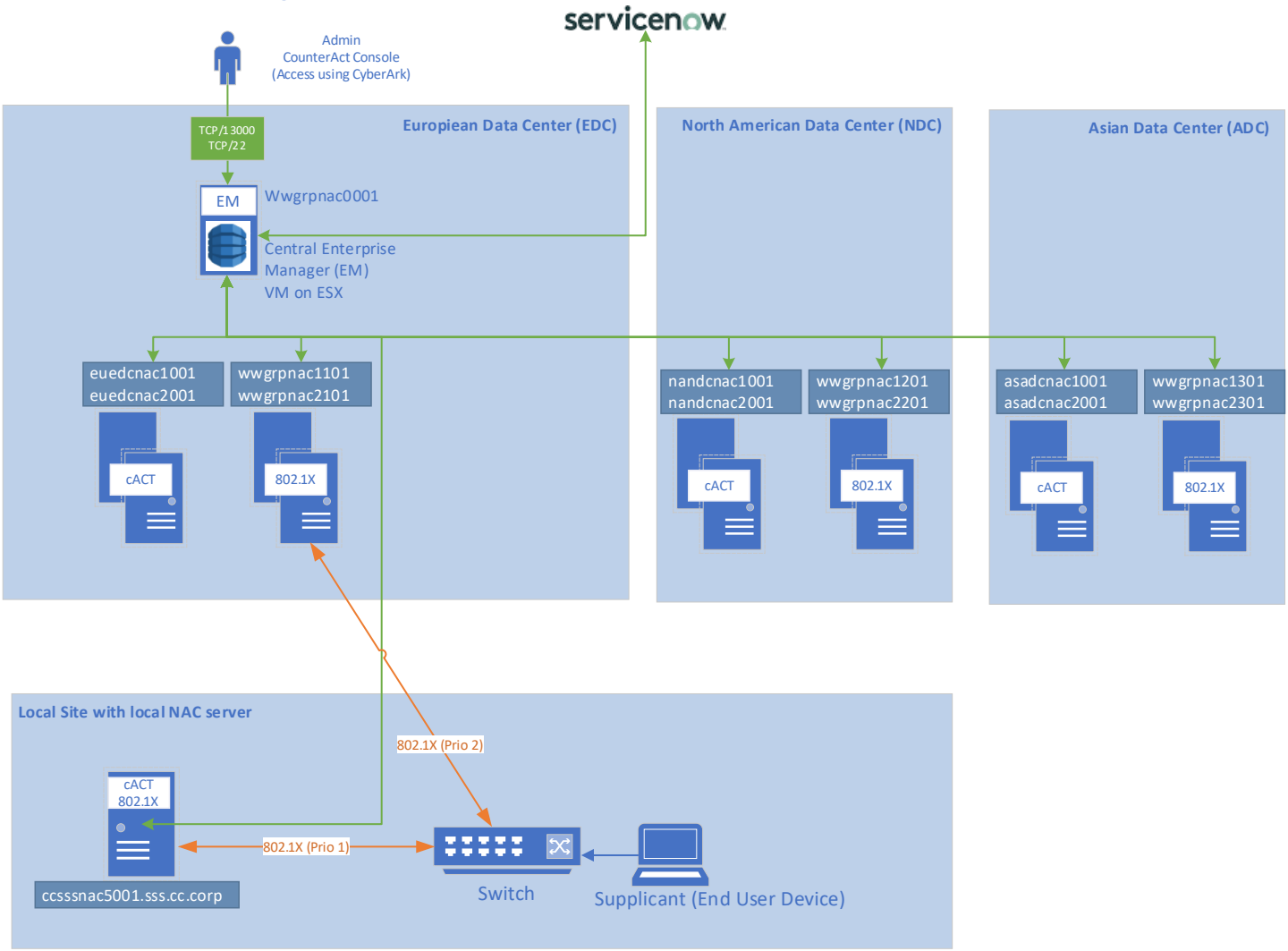
- Faurecia ne disposait d'aucune solution de contrôle d'accès réseau (NAC)Requirement for TISAX / Cardinal audits
- Pas d'inventaire exhaustif des appareils connectés à l'infrastructure réseau qui n'a aucun rapport avec les bases de données suivies avec des indicateurs de sécurité
- Chiffrement (RSE/PGP/Bitlocker)
- Ivanti
- Active Directory
- DLPFaurecia ne disposait d'aucune solution de contrôle d'accès réseau (NAC)
- EDR / SEP (obsolète) / McAfee Virus Scan Enterprise pour le stockage
- Aucune information sur les appareils industriels tels que les automates Siemens, les imprimantes Zebra, Raspberry PI, les lecteurs de codes-barres
- Aucune information sur les appareils externes (n'appartenant pas à l'entreprise)
- Pas de possibilité d'autoriser/refuser la connexion d'appareils au réseau

2. Ce que permet la mise en place du NAC

- Inventaire / détection des appareils connectés à l'infrastructure réseau (indépendant du VLAN)
- Protégez le VLAN des utilisateurs (11) avec une authentification basée sur des certificats (la même méthode que celle actuellement utilisée par l'infrastructure sans fil, mais les serveurs radius seront Forescout)
- Authentification locale (serveurs Radius) pour les sites avec plus de 250 points de terminaison (basée sur SEC-IND)
- Redondance vers le contrôleur de domaine le plus proche en cas de problème entre le serveur local et le contrôleur de domaine
- Repli sur l'état « 802.1X autorisé » dans le cas où AUCUN serveur rayon n'est joignable (panne WAN)
- Repli sur 802.1X autorisé lors de l'implémentation sur les sites pour détecter les « appareils problématiques » locaux de l'entreprise

2.2 L'architecture

NAC Architecture – High level



3. Network Access Control – 802.1X Exigences des clients

Pour procéder au déploiement de NAC et passer de la méthode de détection à la méthode de contrôle, les clients Endpoint ont besoin de nouveaux paramètres de carte réseau déployés par GPO sur TOUS les endpoints Windows dans le monde. Cette GPO :

- Active et démarre automatiquement le service Windows Wired AutoConfig (DOT3SVC)
- Permet au client d'utiliser l'authentification IEEE 802.1X (parler avec les serveurs Radius)
- Choisissez « Certificat client » comme informations d'authentification.
- Vérifier l'identité du serveur en validant le certificat
- Autoriser uniquement l'authentification avec des serveurs NAC conformes à la politique Faurecia (en évitant les faux serveurs 802.1X)
- Sélectionnez des CA Faurecia de confiance
- Repli vers un accès réseau non autorisé (cela permet aux clients de travailler dans des hôtels, des

bureaux à domicile, etc.). L'application de NAC est configurée sur l'équipement réseau, et non sur les clients. Les paramètres permettent aux clients d'utiliser la norme 802.1X, mais n'insistent pas dessus. Ces paramètres sont déployés dans tous les sites Faurecia dans le monde entier