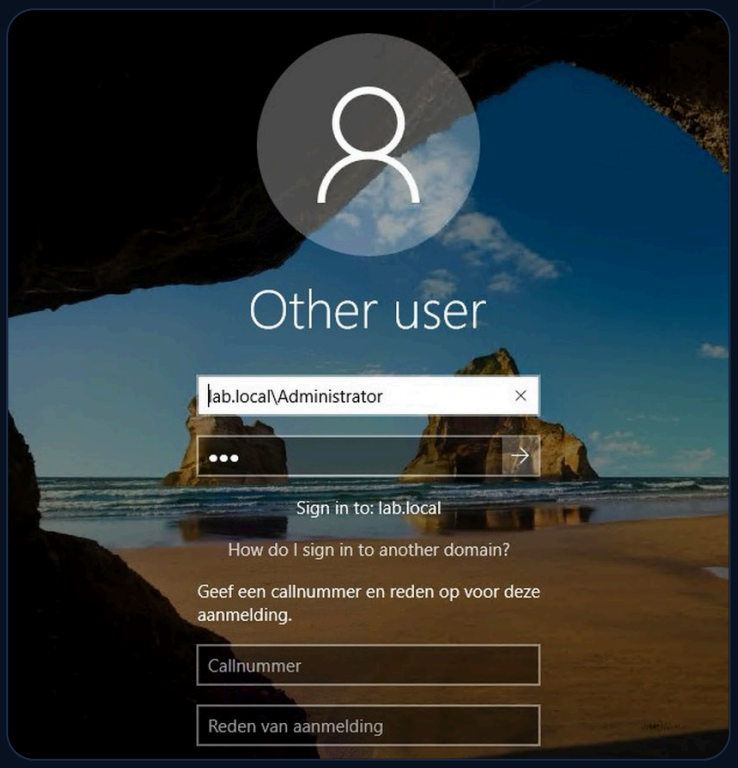
LogonReason

WINDOWS SERVER · TOEGANG

> credential provider voor beheeraanmeldingen

Geen aanmelding zonder reden.

LogonReason vraagt bij elke aanmelding op een server om een callnummer en een reden, en legt beide centraal vast. Wie er inlogde wist je al. Nu weet je ook waarom.



Het echte aanmeldscherm, op Windows Server in een testomgeving.

Console én RDP

Ook bij NLA: geen automatische aanmelding zonder reden.

Altijd beschikbaar

Aanmelden hangt niet af van netwerk, SQL of collector.

Centraal vastgelegd

Via één geharde collector naar SQL Server.

Elke beheeraanmelding met context

Windows legt vast wíe er op een server inlogt en wanneer. Waaróm iemand inlogde staat nergens. Bij een incident of audit begint dan het zoeken. LogonReason maakt de reden onderdeel van de aanmelding zelf.

ZONDER LOGONREASON

Event 4624: gebruiker X logde om 02:14 in op server Y. Geen ticket, geen reden, geen context.

MET LOGONREASON

Dezelfde aanmelding, met callnummer, reden, client-pc en IP-adres. Centraal doorzoekbaar en te koppelen aan het ticket.

Zo werkt het

1

Aanmelden

Console of RDP. Het vertrouwde aanmeldscherm, met twee extra velden.

2

Callnummer + reden

Verplicht, ook bij ontgrendelen. Zonder geldige invoer geen aanmelding.

3

Lokaal gelogd

In een eigen eventkanaal waar alleen het systeem naar mag schrijven.

4

Centraal opgeslagen

Doorgestuurd naar een collector, die het in SQL Server vastlegt.

Wat je krijgt

Console, RDP en NLA

Ook als RDP de inloggegevens al meestuurt, moet de reden worden ingevuld.

Altijd kunnen inloggen

Geen netwerkverkeer tijdens het aanmelden. Een storing in SQL of de collector houdt niemand buiten.

Beheer via GPO

Installatie met MSI, instellingen via een ADMX-template. Het scherm volgt de taal van Windows (26 talen).

Controle op invoer

Callnummer volgens een of meer formaten van je ticketsystemen, reden met een minimale lengte.

Eén bron voor audits

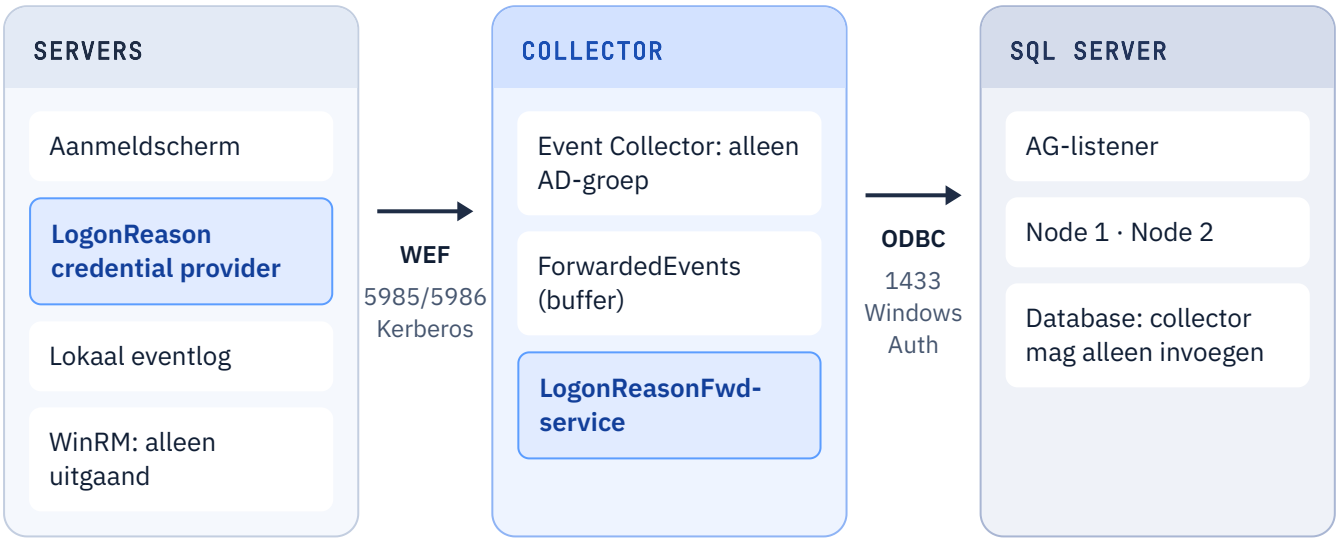
Alle aanmeldingen met reden in SQL Server. Te bevragen en te koppelen aan tickets.

Afwijkingen zichtbaar

Mislukte en afgekeurde pogingen worden gelogd, net als het uitschakelen van LogonReason. Een aanmelding zonder reden valt op naast event 4624.

Eén geharde collector, verder niets

Servers praten niet met de database. Ze sturen hun events naar één collector, en alleen die mag in SQL Server schrijven. Zo blijft de segmentatie strak en is er maar één systeem dat je zwaar hoeft te harden.



Firewallregels

Van	Naar	Poort
Servers	Collector	TCP 5985 / 5986
Collector	AG-listener + nodes	TCP 1433
Servers	SQL Server	**geblokkeerd**

Veilig ontworpen

Afgeschermd eventkanaal
Alleen het systeem schrijft; beheerders lezen. Afgekeurde invoer wordt niet gelogd.

Geen wachtwoorden opgeslagen
Kerberos en het computeraccount, van server tot database.

Database alleen invoegen
De collector kan geen historie lezen, wijzigen of wissen.

Alleen bekende bronnen
De collector accepteert alleen servers uit één AD-groep, en alleen de eigen events.

Gaten worden zichtbaar
Aanmelding (4624) zonder reden valt op, uitschakelen ook (1003).

Nooit buitengesloten
Noodschakelaar via het register, op afstand of offline.

Invoeren in vier stappen

01 **Testen op een VM**
Eerst alleen de provider, met de oude tegels nog zichtbaar. Console, RDP, ontgrendelen en een verlopen wachtwoord doorlopen.

02 **Database en collector inrichten**
SQL-script op het cluster draaien en de collector-MSI installeren. Die richt ook de doorstuurservice en de abonnering in.

03 **Per servergroep uitrollen**
Server-MSI via GPO-softwareinstallatie, instellingen via het ADMX-template, en doorsturen naar de collector.

04 **Detectie aanzetten**
Aanmeldingen zonder reden opsporen door ze te koppelen aan de 4624-events van de domain controllers.

Instelbaar via GPO

Aan / uit	noodschakelaar
Callnummer	een of meer formaten
Reden	min. en max. lengte
Teksten	eigen tekst, of taal van Windows
Extra tegels	bijv. smartcard

Benodigdheden

Servers	Windows Server, in AD
Collector	1 Windows Server
Database	SQL Server (AG optioneel)
Driver	ODBC 18 + VC++-runtime (collector)
Installatie	2 MSI's + ADMX, geen agents

Eerlijk over de grenzen
LogonReason geldt voor interactieve aanmeldingen. PowerShell remoting, PsExec, geplande taken en services gaan buiten het aanmeldscherm om. Een lokale beheerder kan de provider uitschakelen. Daarom hoort de koppeling met de 4624-events erbij: dan valt omzeilen op.

MEER INFORMATIE
Martijn Peeters
info@mpeeters.nl
mpeeters.nl