

ADC configureren met gebeurtenislogboekverzamelaar en domeinen

Inhoud

[Inleiding](#)

[Configuratieopties](#)

[Belangrijke overwegingen:](#)

[Er zijn enkele bekende beperkingen voor deze implementatiemodus:](#)

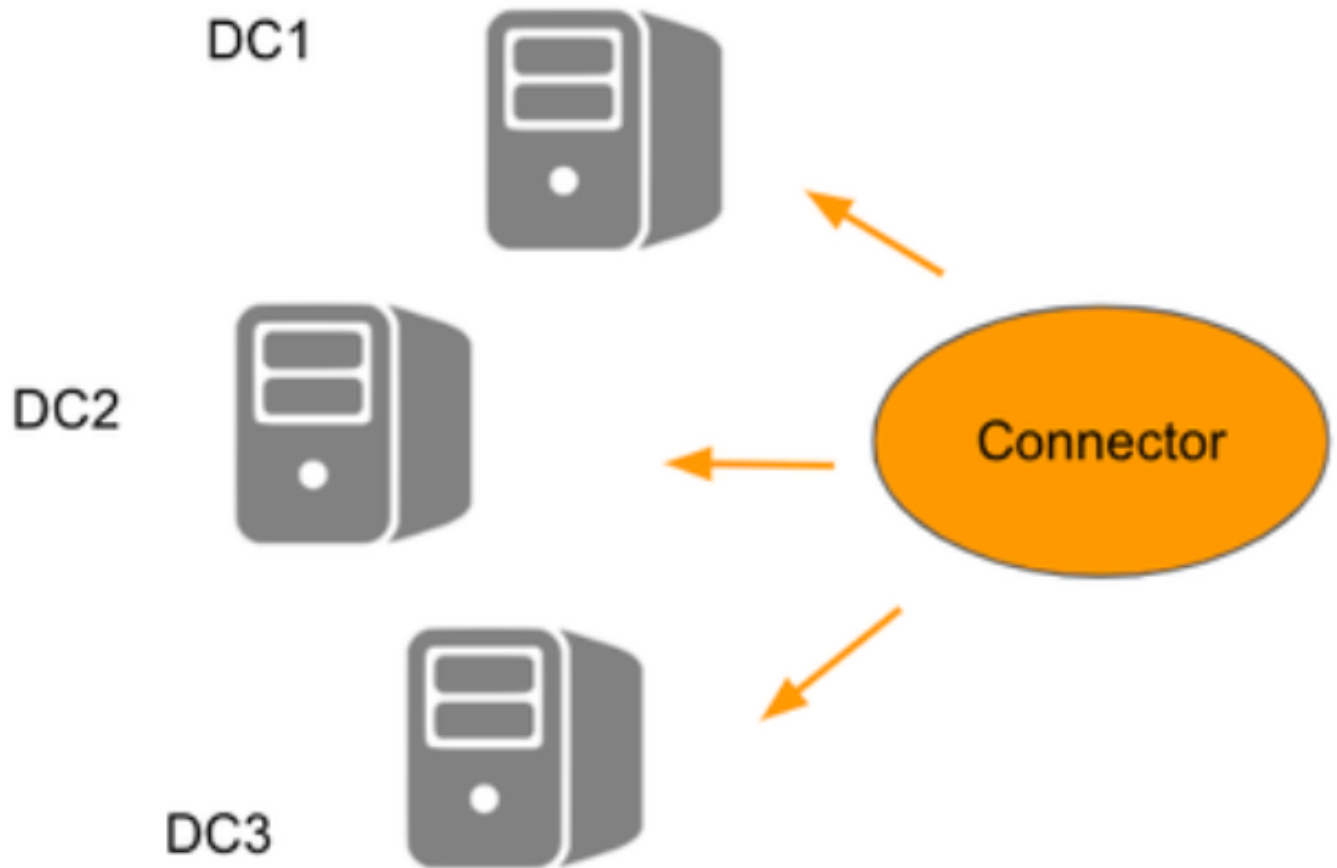
Inleiding

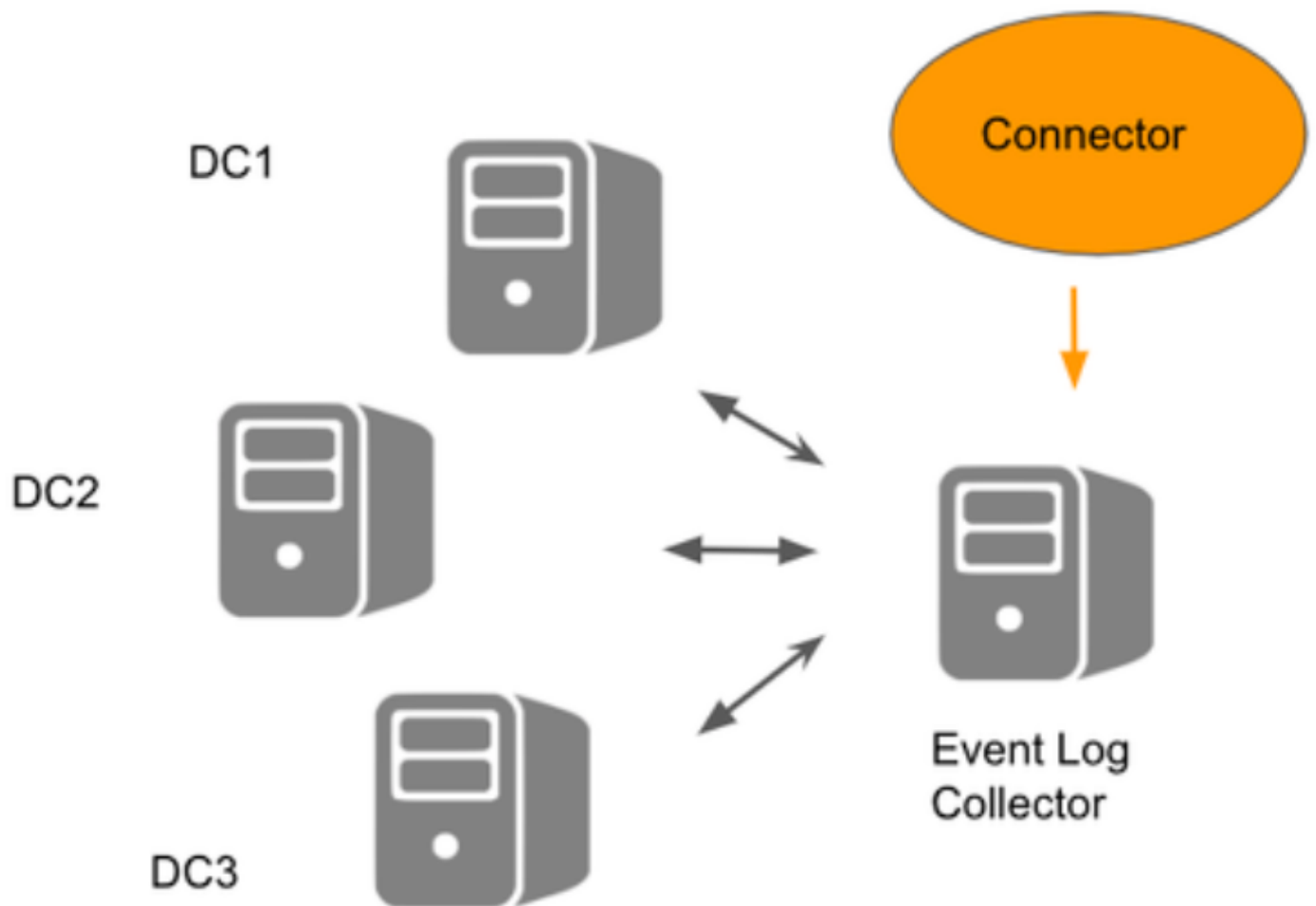
In dit document wordt beschreven hoe u de Active Directory Connector (ADC) configureert met Event Log Collector en Domains.

Configuratieopties

Er zijn twee instelmogelijkheden beschikbaar voor het gebruik van de Active Directory:

1. Domeincontrollers registreren: hierbij wordt gebruikgemaakt van Virtual Appliances (VA) en de AD-connector, waarbij de AD-connector rechtstreeks communiceert met alle geregistreerde domeincontrollers (DC's).
2. **Gebeurtenislogboekverzamelaar:** deze installatie omvat het domein, de VA en de AD-connector. In dit scenario verzendt Windows Event Log Forwarding informatie van de DC's naar een centrale verzamelserver voor gebeurtenislogboeken. De AD-connector communiceert dan alleen met deze centrale server, niet met de DC's



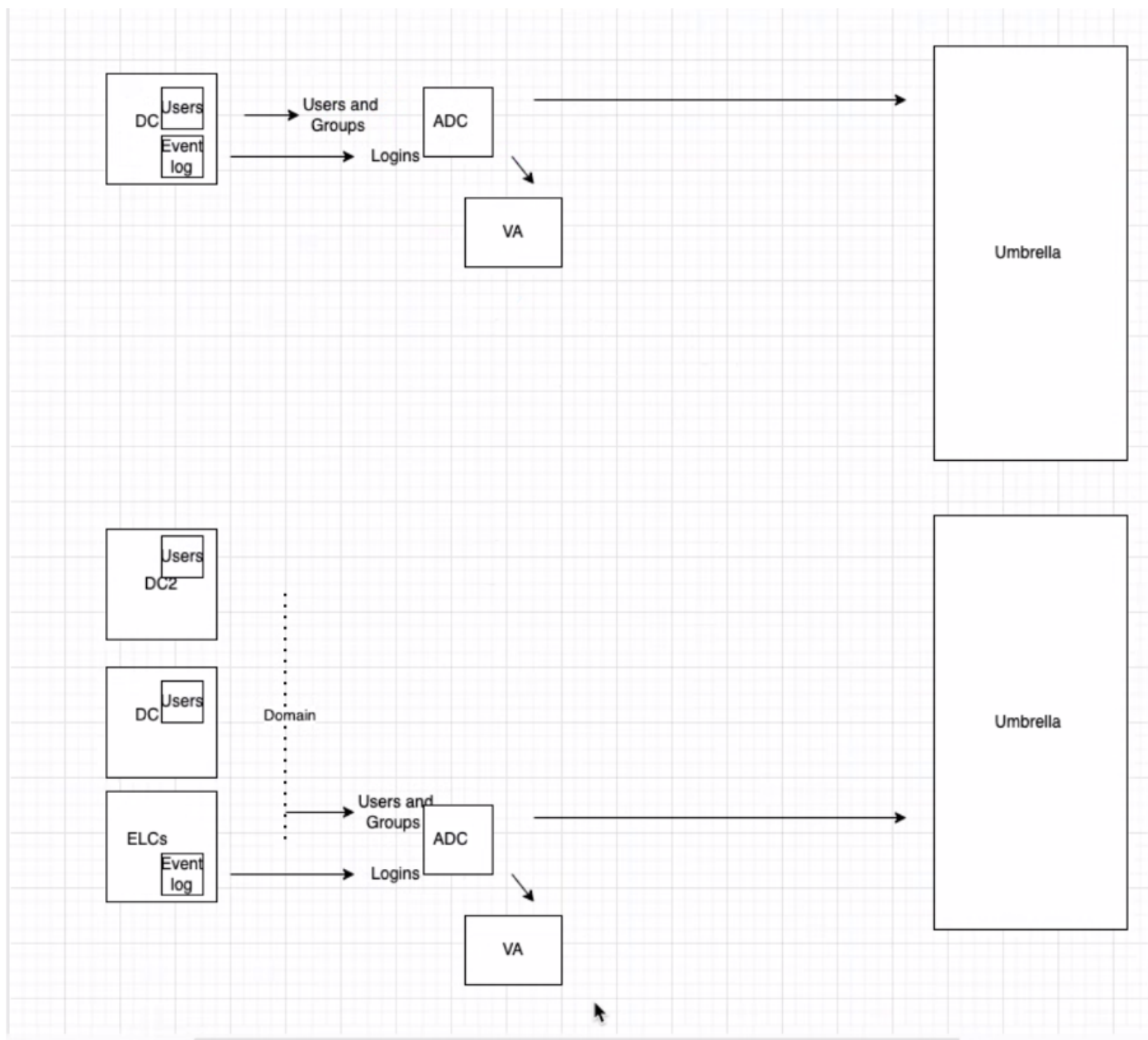


22062473502228

Umbrella EventLogReader ←
Windows Event Log Forwarding ←

22062518240276

Let op: Domeincontrollers registreren en domeinen toevoegen zijn verschillende processen.



22062518241684

1. Om de configuratie te starten in het Umbrella-dashboard, navigeert u naar Implementaties > Configuratie > Sites en Active Directory en klikt u op Toevoegen. Selecteer Windows Event Log Collector en klik op Volgende.

Add Windows Event Log Collector

Hostname

wef

Log Path

ForwardedEvents

Internal IP

10.10.105.11

Domain

adclab.local

Site

Default Site

CANCEL

PREVIOUS

SAVE

22062473507220

2. Klanten kunnen de eigenschappen van het logbestand controleren (in Windows Event Viewer) om de naam van het logbestand te achterhalen. Houd er rekening mee dat de naam van het logbestand moet worden ingevoerd zonder de extensie .evtx of de volledige padgegevens.

Log Properties - Forwarded Events (Type: Operational)

×

General Subscriptions

Full Name: ForwardedEvents

Log path: %SystemRoot%\System32\Winevt\Logs\ForwardedEvents.evtx

22062518244756

Belangrijke overwegingen:

Om de Connector correct te laten functioneren, is het noodzakelijk om door te gaan met de normale implementatiestappen:

1. Registreer een 'Domein' op de pagina 'Sites en Active Directory' met het oog op gebruikersprovisioning. Dit is nodig omdat er geen geregistreerde DC is om

gebruikers/groepen van te synchroniseren.

2. Implementeer 'Virtuele apparaten'.

Er zijn enkele bekende beperkingen voor deze implementatiemodus:

- De connector kan in een foutstatus worden weergegeven, zelfs als deze goed werkt.

Om de AD-connector efficiënt te laten werken, zijn bepaalde machtigingen vereist. U kunt deze machtigingen hier bekijken: Vereiste machtigingen voor de OpenDNS_Connector-gebruiker.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.