

ADC mit Ereignisprotokollsammler und Domänen konfigurieren

Inhalt

[Einleitung](#)

[Konfigurationsoptionen](#)

[Wichtige Überlegungen:](#)

[Es gibt einige bekannte Einschränkungen für diesen Bereitstellungsmodus:](#)

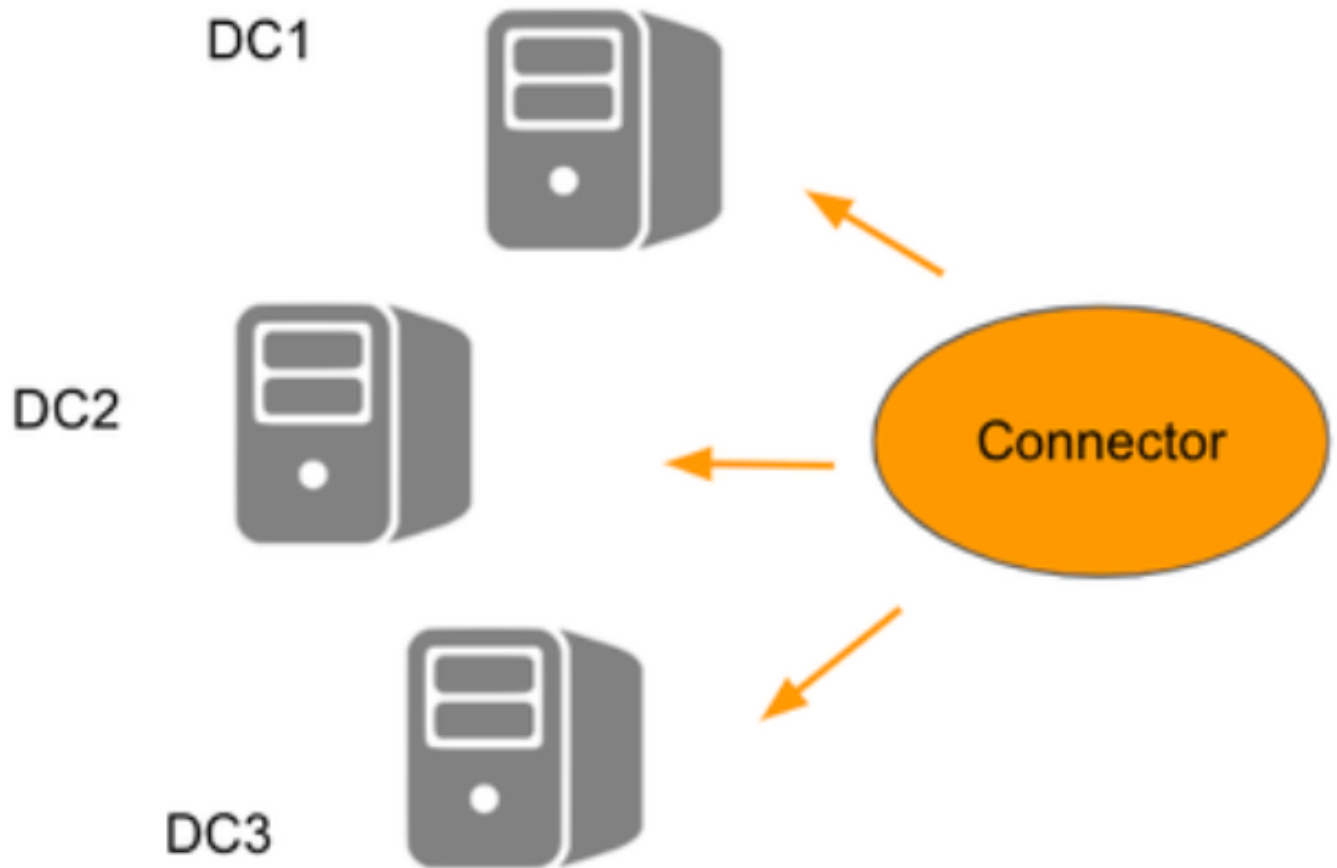
Einleitung

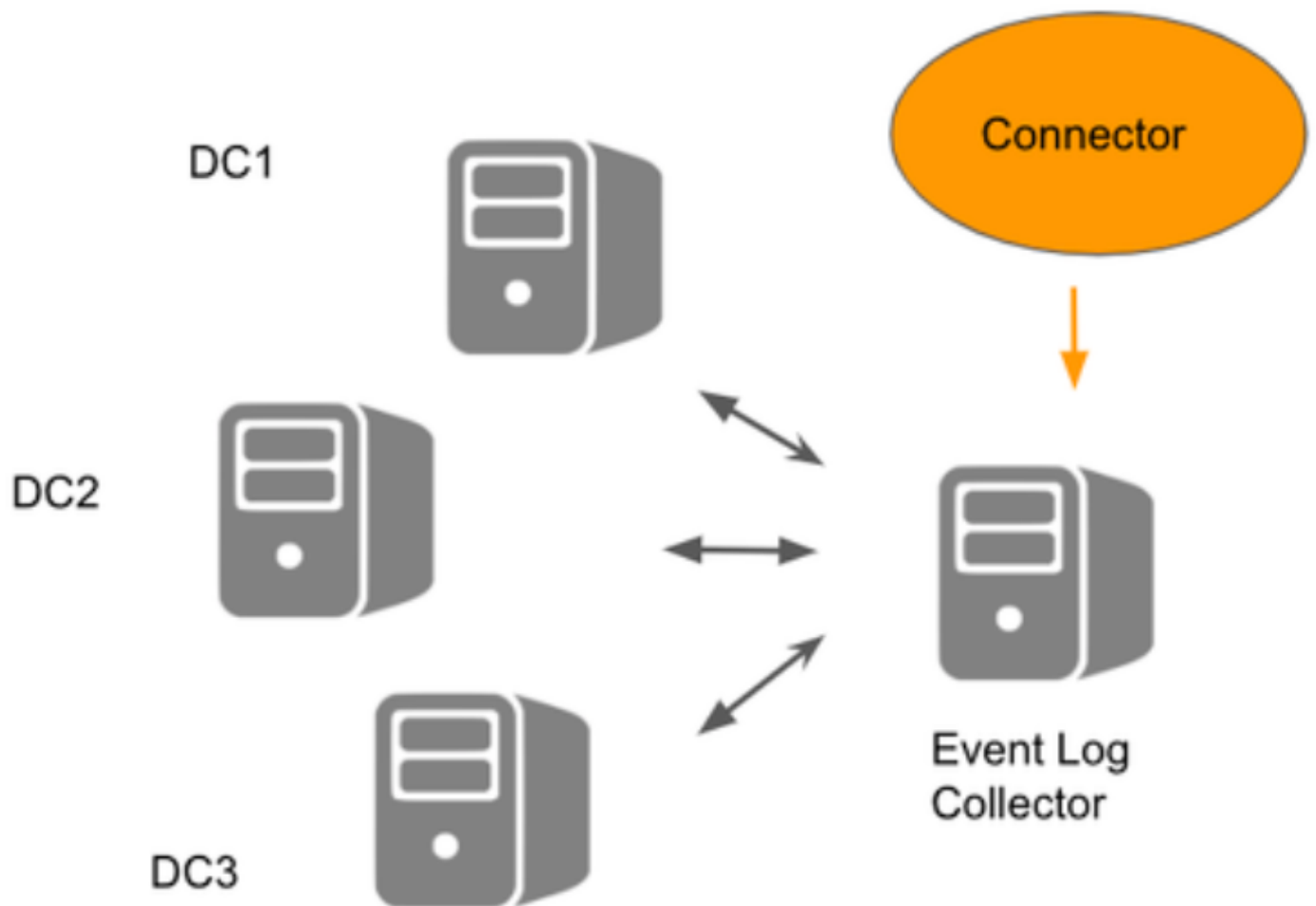
In diesem Dokument wird beschrieben, wie der Active Directory-Connector (ADC) mit der Ereignisprotokollsammlung und Domänen konfiguriert wird.

Konfigurationsoptionen

Für die Verwendung von Active Directory stehen zwei Setup-Optionen zur Verfügung:

1. Domänencontroller werden registriert: Hierzu werden virtuelle Appliances (VA) und der AD-Connector verwendet, wobei der AD-Connector direkt mit allen registrierten Domänencontrollern (DCs) kommuniziert.
2. **Event Log Collector:** Diese Konfiguration umfasst die Domäne, die VA und den AD Connector. In diesem Szenario sendet die Windows-Ereignisprotokollweiterleitung Informationen von den Domänencontrollern an einen zentralen Ereignisprotokollsammlungsserver. Der AD Connector kommuniziert dann nur mit diesem zentralen Server, nicht mit den Rechenzentren.



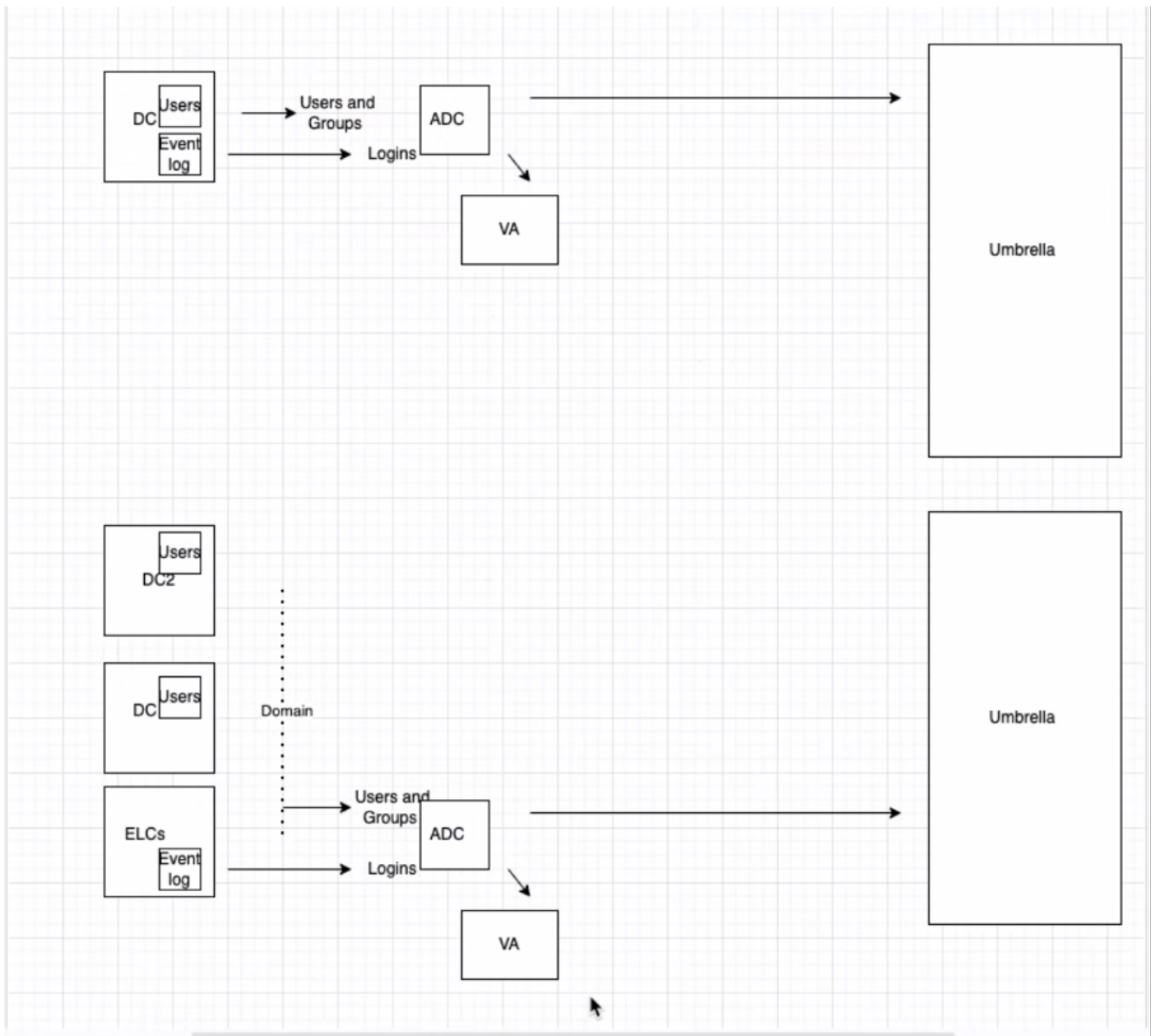


22062473502228

Umbrella EventLogReader 
Windows Event Log Forwarding 

22062518240276

Bitte beachten: Das Registrieren von Domänencontrollern und das Hinzufügen von Domänen sind unterschiedliche Prozesse.



22062518241684

1. Um die Konfiguration im Umbrella Dashboard zu starten, navigieren Sie zu Deployments > Configuration > Sites and Active Directory, und klicken Sie auf Add. Wählen Sie Windows-Ereignisprotokollsammler aus, und klicken Sie auf Weiter.

Add Windows Event Log Collector

Hostname

Log Path

Internal IP

Domain

Site

CANCEL

PREVIOUS

SAVE

22062473507220

2. Kunden können die Eigenschaften der Protokolldatei (in der Windows-Ereignisanzeige) überprüfen, um den Namen des Protokolls herauszufinden. Beachten Sie, dass der Name der Protokolldatei ohne die Erweiterung .evtx oder vollständige Pfadangaben eingegeben werden muss.

Log Properties - Forwarded Events (Type: Operational)



General Subscriptions

Full Name: ForwardedEvents

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

22062518244756

Wichtige Überlegungen:

Damit der Connector ordnungsgemäß funktioniert, müssen die üblichen Bereitstellungsschritte ausgeführt werden:

1. Registrieren Sie eine Domäne auf der Seite "Sites und Active Directory", um Benutzer

bereitzustellen. Dies ist erforderlich, da kein registrierter Domänencontroller zum Synchronisieren von Benutzern/Gruppen vorhanden ist.

2. Bereitstellen von 'virtuellen Appliances'.

Es gibt einige bekannte Einschränkungen für diesen Bereitstellungsmodus:

- Der Connector kann in einem Fehlerzustand angezeigt werden, selbst wenn er ordnungsgemäß funktioniert.

Damit der AD-Connector effizient funktioniert, sind bestimmte Berechtigungen erforderlich. Sie können diese Berechtigungen hier überprüfen:[Erforderliche Berechtigungen für den OpenDNS_Connector-Benutzer](#).

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.