ISE 2.2
Primary

ISE 2.2
Secondary

Member Server
P190WEC01
(MS 2016)

Domain Controller
10.x.x.101
(#1 Domain)

Domain Controller
10.x.x.102
(#1 Domain)

Domain Controller
10.x.x.201
(#2 Domain)

Domain Controller
10.x.x.202
(#2 Domain)

**Based on the recommendation from Aaron Woland
CiscoLive 2017 – BRKSEC-3697
Log Forwarding to Increase Scale**

ISE 2.2
Primary

ISE 2.2
Secondary
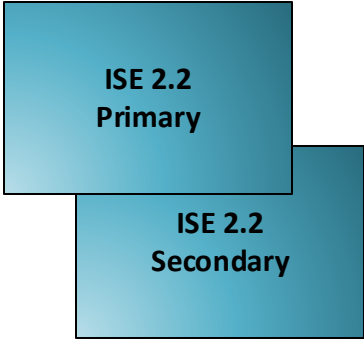
Active Directory

	Edit	Add	Delete	Node View	Advanced Tools ▾	Scope Mode

☐	Join Point Name ▲	Active Directory Domain
☐	Remote Child	#2 domain
☐	Corporate	Main domain
☐	Corporate Child	#1 domain

Connection	Whitelisted Domains	PassiveID	Groups	Attributes	Advanced Settings

* Join Point Name   Corporate   ⓘ

* Active Directory Domain   Abcdef.com   ⓘ

Join   Leave   Test User   Diagnostic Tool   Refresh Table

☐	ISE Node ▲	ISE Node Role	Status	Domain Controller	Site
☐	Ise-primary.abcdef.com	PRIMARY	☑ Operational	domaincontroller1.abcdef.com	Corporate
☐	Ise-secondary.abcdef.com	SECONDARY	☑ Operational	domaincontroller2.abcdef.com	Corporate

Connection	Whitelisted Domains	PassiveID	Groups	Attributes	Advanced Settings

* Join Point Name   Corporate Child   ⓘ

* Active Directory Domain   CorporateChild.abcdef.com   ⓘ

Join   Leave   Test User   Diagnostic Tool   Refresh Table

☐	ISE Node ▲	ISE Node Role	Status	Domain Controller	Site
☐	Ise-primary.abcdef.com	PRIMARY	☑ Operational	domaincontroller1.abcdef.com	Corporate
☐	Ise-secondary.abcdef.com	SECONDARY	☑ Operational	domaincontroller2.abcdef.com	Corporate

Connection	Whitelisted Domains	PassiveID	Groups	Attributes	Advanced Settings

PassiveID Domain Controllers

Rows/Page 2 ▾ ⫷ ◀ 1 /1

Refresh   Edit   Trash   Add DCs   Use Existing Agent   Config WMI   Add Agent

☐	Domain	DC Host	Site	IP Address	Monitor Using
☐	CorporateChild.abcdef.com	domaincontroller1.abcdef.com	Corporate	10.x.x.101	P190WEC01
☐	CorporateChild.abcdef.com	domaincontroller2.abcdef.com	Corporate	10.x.x.102	P190WEC01

Agents

Rows/Page 1 ▾ ⫷ ◀ 1 /1 ▶ ⫸ Go   1 Total

Refresh   Add   Duplicate   Trash ▾   Edit   Download Agent   Upload Agent   Filter ▾

☐	Name	Host	Monitoring
☐	P190WEC01	P190WEC01.corporatechild.abcdef.com	domaincontroller1.abcdef.com, domaincontroller2.abcdef.com

**Member Server
P190WEC01
(MS 2016)**

- Member Server belongs in the root domain (ABCDEF.COM)
- PassiveID Agent installed manually
- DC 1 – 4 feeding Security Logs
- Configured using the MS TechNet document (Quick and Dirty Large Scale Eventing for Windows)

- https://blogs.technet.microsoft.com/wincat/2008/08/11/quick-and-dirty-large-scale-eventing-for-windows/

-

Event Viewer	P190WEC01.ABCDEFG.COM
Custom Views	
Windows Logs	
Application	
Security	
Setup	
System	
Forwarded Events	
Applications and Services Logs	
Hardware Events	
Internet Explorer	
Key Management Service	
Microsoft	
PICAgentLog	
Windows PowerShell	

Forwarded Events Number of events: 117,666 (!) New events available

Level	Date and Time	Source	Event ID	Task Category	Log
(i) Information	8/21/2017 2:11:58 PM	Microsoft Windows security auditing.	4769	Kerberos Service Ticket Operations	Sec
(i) Information	8/21/2017 2:11:57 PM	Microsoft Windows security auditing.	4769	Kerberos Service Ticket Operations	Sec
(i) Information	8/21/2017 2:11:57 PM	Microsoft Windows security auditing.	4769	Kerberos Service Ticket Operations	Sec
(i) Information	8/21/2017 2:11:57 PM	Microsoft Windows security auditing.	4769	Kerberos Service Ticket Operations	Sec
(i) Information	8/21/2017 2:11:57 PM	Microsoft Windows security auditing.	4769	Kerberos Service Ticket Operations	Sec
(i) Information	8/21/2017 2:11:56 PM	Microsoft Windows security auditing.	4769	Kerberos Service Ticket Operations	Sec
(i) Information	8/21/2017 2:11:55 PM	Microsoft Windows security auditing.	4769	Kerberos Service Ticket Operations	Sec

Event 4769, Microsoft Windows security auditing.

General | Details

A Kerberos service ticket was requested.

Account Information:
    Account Name: BarneyFife@ChildDomain.ABCDE.COM
    Account Domain: ChildDomain.ABCDE.COM
    Logon GUID: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx