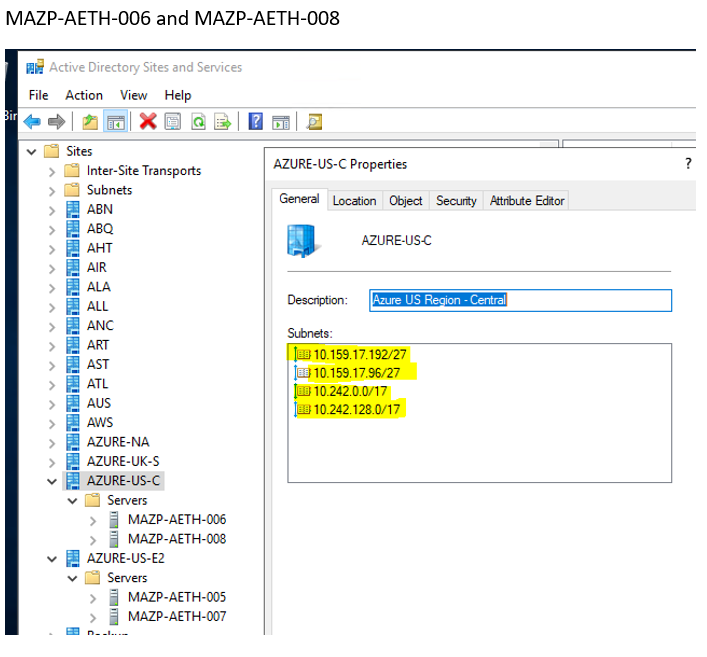
|  |
| --- |
| **Audit Name: Active Directory**  **Audit Number: 21121**  **Prepared by: Seun Mafi**  **Date Completed: 1/19/2022** |

|  |  |
| --- | --- |
| Control & Sample Information | |
| Control | C1.1 – Domain Controller Availability |
| Sample Number | 100% of PSS/Retail AD Sites and Services, and HCB AD Sites and Services were tested to determine adequacy and effectiveness of this control |
| Supporting Documentation Received From | James W. Rose (Senior Engineer Advisor) |
| Received Date | 12/22/2021, 1/12/2022 |
| Purpose of the Test | The purpose of this test is to ensure that domain controller replication / redundancy have been implemented on all the domains and domain controllers are configured to pick up loads of users / workstation of another domain controller in a different region when there is a system malfunction. |
| Source Files | [Task13199 – Security of Domain Controllers DC Redundancy](https://cvshealth.auditboardapp.com/download?file_id=156438&name=Task13199%20-%20Security%20of%20Domain%20Controllers%20DC%20Redundancy.docx)  [Task 14777 – Domain Controller Availability](https://cvshealth.auditboardapp.com/download?file_id=155430&name=Task-14777%20-%20C1.1%20-%20Domain%20Controller%20Availability%20.docx)  [Microsoft - Finding a Domain Controller](https://cvshealth.auditboardapp.com/download?file_id=156478&name=Microsoft_Finding%20a%20Domain%20Controller.pdf)  [Microsoft – Active Directory Collection](https://cvshealth.auditboardapp.com/download?file_id=156778&name=Microsoft%20-%20Active%20Directory%20Collection.pdf) |

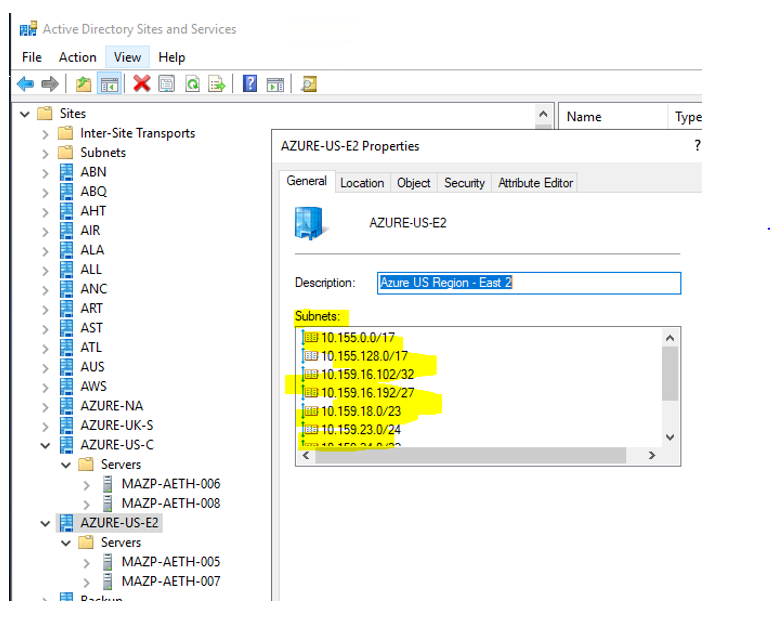
**Attribute 1: Evidence of Configuration setting showing domain controller replication/redundancy have been implemented on all the domains.**

On 12,22,2021, IA received from Jim Rose (Senior Engineering Advisor) evidence showing the Active directory site design which include the shared services hub containing the Azure US Region Central and East both configured to replicate data simultaneously. Azure US Region Central and East are sites containing domain controllers used for authentication. According to the information provided by Jim ([Task 14777 – Domain Controller Availability](https://cvshealth.auditboardapp.com/download?file_id=155430&name=Task-14777%20-%20C1.1%20-%20Domain%20Controller%20Availability%20.docx)), per Microsoft AD default policy as outlined in the automatic site coverage section of ([Microsoft\_Finding a Domain Controller](https://cvshealth.auditboardapp.com/download?file_id=156478&name=Microsoft_Finding%20a%20Domain%20Controller.pdf)) document, by default, each domain controller checks all sites in the forest and then checks the replication matrix. Furthermore, to ensure that a domain controller can be located in the site closest to a client computer, windows automatically attempt to register a domain controller in every site. The algorithm that is used to accomplish automatic site coverage determines how one site can cover another site when no domain controller exists in the second site. In addition, in the replication technologies section of the ([Microsoft – Active Directory Collection](https://cvshealth.auditboardapp.com/download?file_id=156778&name=Microsoft%20-%20Active%20Directory%20Collection.pdf)) document provided by Microsoft, it states that objects in the directory are distributed among the domain controllers in a forest, and all domain controllers can be updated directly. Hence, following these defined default configuration by Microsoft, it is evident that the CVS AD environment containing Azure Central and East are configured to have failover/redundancy. Jim Rose provided the listing of Domain controller contained in each AD site. *See evidence below:*

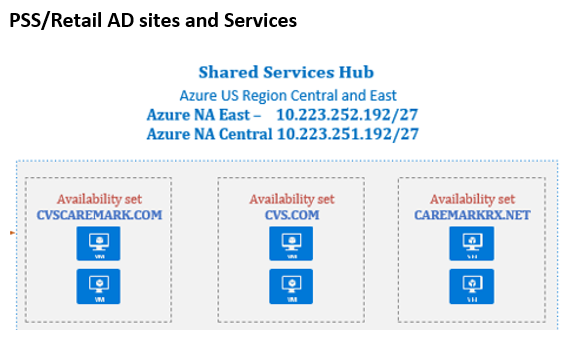
1. Azure US Central

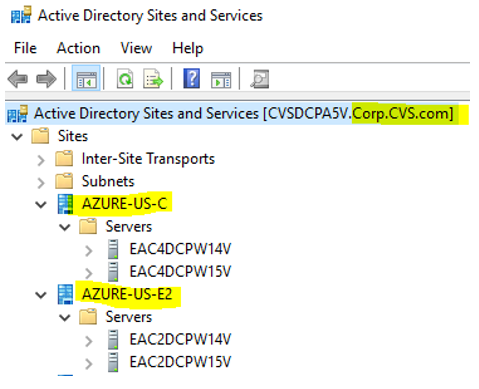
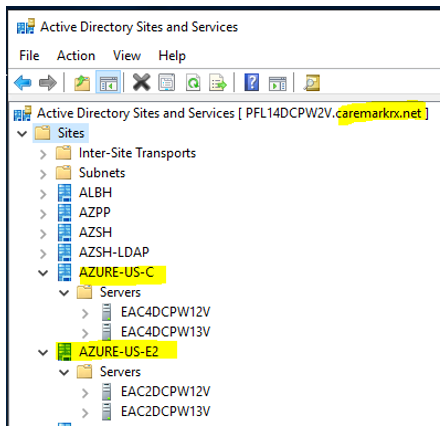
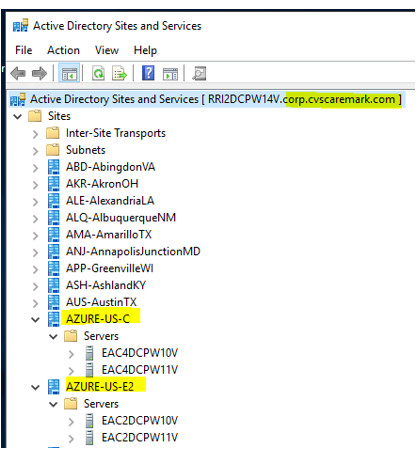


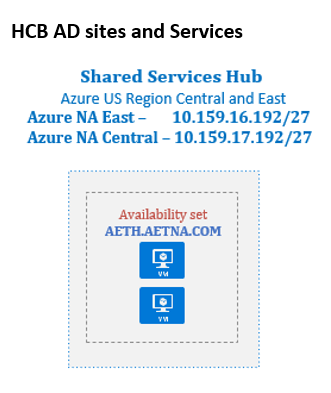
1. Azure US East

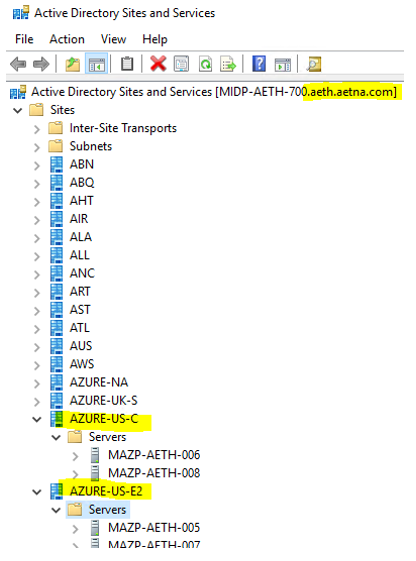


Following this information, Jim Rose (Senior Engineering Advisor) provided the Azure design configuration showing replication / redundancy on both the Azure US Central and Azure US East AD sites for PSS/Retail AD Sites and Services, and HCB AD Sites and Services. ([Task13199 – Security of Domain Controllers DC Redundancy](https://cvshealth.auditboardapp.com/download?file_id=156438&name=Task13199%20-%20Security%20of%20Domain%20Controllers%20DC%20Redundancy.docx)). *See evidence below:*

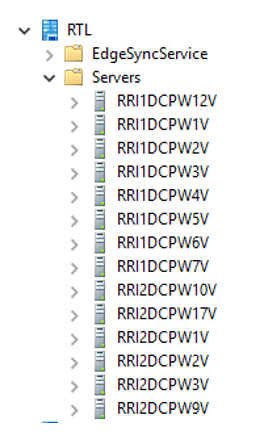
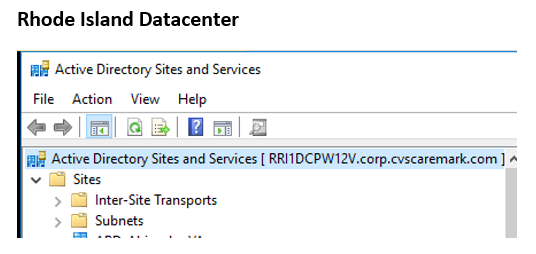


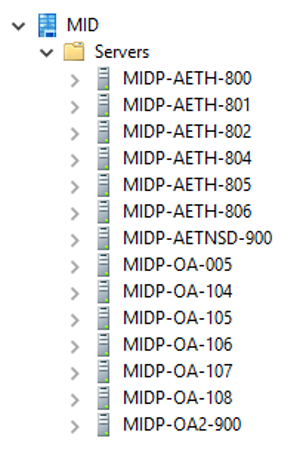
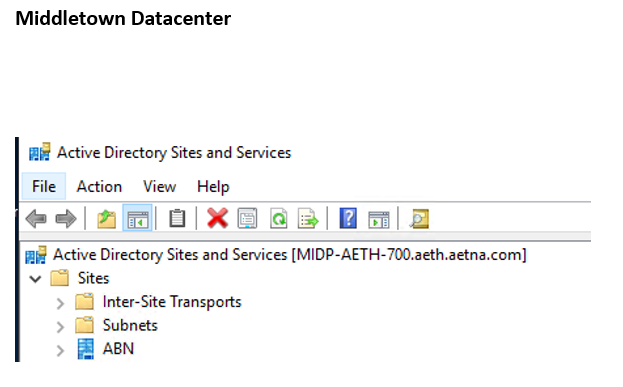






In the document ([Task13199 – Security of Domain Controllers DC Redundancy](https://cvshealth.auditboardapp.com/download?file_id=156438&name=Task13199%20-%20Security%20of%20Domain%20Controllers%20DC%20Redundancy.docx)) provided by Jim Rose (Senior Engineering Advisor), IA also noted evidence showing the datacenters in which both the CVS and Aetha AD Sites reside. *See evidence below:*



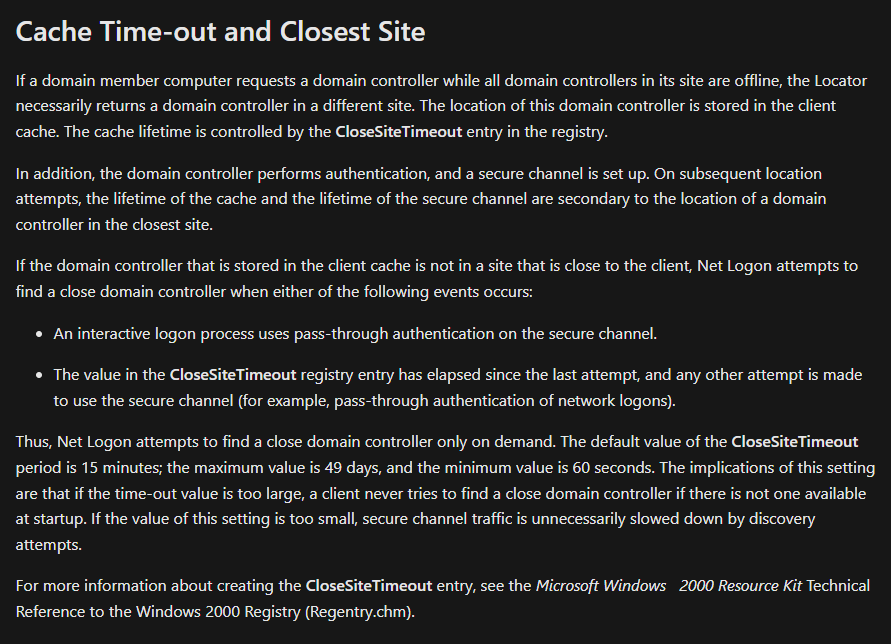


IA gained assurance that domain controller replication/redundancy are implemented on all the domains.

Attribute satisfied.

**Attribute 2: Evidence showing that Domain Controller is configured to pick up load of users / workstations of another domain controller in a different region when there is a system malfunction.**

According to the information provided by Jim Rose (Senior Engineering Advisor) ([Task 14777 – Domain Controller Availability](https://cvshealth.auditboardapp.com/download?file_id=155430&name=Task-14777%20-%20C1.1%20-%20Domain%20Controller%20Availability%20.docx)), when a client searching for a domain controller receives the list of domain controller IP addresses from DNS, the client begins querying the domain controllers in turn to find out which domain controller is available and appropriate. If a domain controller would fail, the clients in those network will then search for the next best responding domain controller. IA also noted given that the Active Directory environment is built in the Microsoft azure platform, the AD infrastructure team utilizes the default configurations as defined by Microsoft. In the Cache Time-out and Closest Site section of the ([Microsoft\_Finding a Domain Controller](https://cvshealth.auditboardapp.com/download?file_id=156478&name=Microsoft_Finding%20a%20Domain%20Controller.pdf)) document, IA noted that if the domain controller that is stored in the client cache is not in a site that is close to the client, net logon attempts to find a close domain controller. This scenario outlined is similar in occurrence and execution as to when a domain controller does not respond, hence enabling a closer domain controller to pick up the load and continue functions. *See evidence below:*



IA observed that although the AD infrastructure utilizes the pre-defined configured as characterized by Microsoft, there was no sufficient evidence in the form of a system generated configuration/setting in the AD environment that shows domain controllers can pick up load of users/workstation of another controller in a different region when there is a system outage/malfunction; however, IA gains comfort in the replication technology of Domain controllers as being sufficient to distribute load across different domain controllers in a forest in an event where there is system malfunction.

Attribute satisfied.

**Conclusion:**

After testing the evidence and artifacts provided, IA gained assurance that configuration settings show domain controller replication / redundancy have been implemented on all the domains and domain controllers are configured to pick up load of users/workstations of another domain controller in a different region should there be a system outage/malfunction; however, IA also observed that there was no system generated setting in the AD environment that evidences such scenario configured.