



Microsoft Active Directory As Built Report

ACME Inc.

Author: Bugs Bunny
Date: Saturday, April 13, 2024
Version: 1.0

Table of Contents

1 SEVENKINGDOMS.LOCAL	5
1.1 Forest Configuration.	5
1.1.1 Forest Diagram.....	6
1.1.2 Certificate Authority	6
1.1.3 Optional Features	7
1.1.4 Replication	7
1.1.4.1 Sites.....	7
1.1.4.2 Site Inventory Diagram.	8
1.1.4.3 Inter-Site Transports.....	8
1.1.4.3.1 IP.....	9
1.1.4.3.1.1 Site Links.....	9
1.1.4.4 Sysvol Replication.....	9
2 AD Domain Configuration.....	9
2.1 SEVENKINGDOMS.LOCAL.....	9
2.1.1 FSMO Roles.....	10
2.1.2 Domain and Trusts	11
2.1.3 Domain Object Stats	12
2.1.4 Status of Users Accounts	15
2.1.5 Privileged Groups	15
2.1.6 Status of Computer Accounts	18
2.1.7 Operating Systems Count.....	18
2.1.8 Default Domain Password Policy	18
2.1.9 Windows LAPS.....	19
2.1.10 Foreign Security Principals.....	19
2.1.11 Health Checks	20
2.1.12 Domain Controllers	23
2.1.12.1 KINGSLANDING	23
2.1.12.2 DNS IP Configuration.....	24
2.1.12.3 NTDS Information	25
2.1.12.4 Time Source Information	25
2.1.12.5 SRV Records Status.....	25
2.1.12.6 File Shares.....	25
2.1.12.7 Roles	26
2.1.12.8 DC Diagnostic.....	26

Microsoft Active Directory As Built Report - v1.0

2.1.12.9 Infrastructure Services	28
2.1.13 Replication Connection	29
2.1.14 Replication Status	30
2.1.15 Group Policy Objects	30
2.1.15.1 Central Store Repository	31
2.1.16 Organizational Units	31
2.2 NORTH.SEVENKINGDOMS.LOCAL	32
2.2.1 FSMO Roles	32
2.2.2 Domain and Trusts	33
2.2.3 Domain Object Stats	34
2.2.4 Status of Users Accounts	37
2.2.5 Privileged Groups	37
2.2.6 Status of Computer Accounts	39
2.2.7 Operating Systems Count.....	39
2.2.8 Default Domain Password Policy	39
2.2.9 Foreign Security Principals	40
2.2.10 Health Checks	40
2.2.11 Domain Controllers	43
2.2.11.1 WINTERFELL	43
2.2.11.2 DNS IP Configuration.....	45
2.2.11.3 NTDS Information	45
2.2.11.4 Time Source Information	45
2.2.11.5 SRV Records Status.....	46
2.2.11.6 Roles	46
2.2.11.7 DC Diagnostic.....	46
2.2.11.8 Infrastructure Services	48
2.2.12 Replication Connection	49
2.2.13 Replication Status	49
2.2.14 Group Policy Objects	50
2.2.14.1 Central Store Repository	51
2.2.15 Organizational Units	51
3 DNS Configuration	52
3.1 SEVENKINGDOMS.LOCAL.....	52
3.1.1 Infrastructure Summary.....	52
3.1.1.1 Application Directory Partition.....	52

Microsoft Active Directory As Built Report - v1.0

- 3.1.1.2 Response Rate Limiting (RRL)52
- 3.1.1.3 Scavenging Options53
- 3.1.1.4 Forwarder Options53
- 3.1.1.5 Root Hints53
- 3.1.1.6 Zone Scope Recursion54
- 3.1.2 KINGSLANDING DNS Zones54
 - 3.1.2.1 Zone Delegation54
 - 3.1.2.2 Reverse Lookup Zone.....54
 - 3.1.2.3 Conditional Forwarder55
 - 3.1.2.4 Zone Scope Aging55
- 3.2 NORTH.SEVENKINGDOMS.LOCAL55
 - 3.2.1 Infrastructure Summary.....55
 - 3.2.1.1 Application Directory Partition.....55
 - 3.2.1.2 Response Rate Limiting (RRL)56
 - 3.2.1.3 Scavenging Options56
 - 3.2.1.4 Forwarder Options56
 - 3.2.1.5 Root Hints57
 - 3.2.1.6 Zone Scope Recursion57
 - 3.2.2 WINTERFELL DNS Zones57
 - 3.2.2.1 Reverse Lookup Zone.....57
 - 3.2.2.2 Conditional Forwarder58
 - 3.2.2.3 Zone Scope Aging58

1 SEVENKINGDOMS.LOCAL

The following section provides a summary of the Active Directory Infrastructure configuration for SEVENKINGDOMS.LOCAL.

1.1 Forest Configuration.

The following section provides a summary of the Active Directory Forest Information.

Forest Name	sevenkingdoms.local
Forest Functional Level	Windows2016Forest
Schema Version	ObjectVersion 88, Correspond to Windows Server 2019
Tombstone Lifetime (days)	180
Domains	north.sevenkingdoms.local; sevenkingdoms.local
Global Catalogs	kingslanding.sevenkingdoms.local; winterfell.north.sevenkingdoms.local
Domains Count	2
Global Catalogs Count	2
Sites Count	1
Application Partitions	DC=DomainDnsZones,DC=north,DC=sevenkingdoms,DC=local DC=ForestDnsZones,DC=sevenkingdoms,DC=local DC=DomainDnsZones,DC=sevenkingdoms,DC=local
PartitionsContainer	CN=Partitions,CN=Configuration,DC=sevenkingdoms,DC=local
SPN Suffixes	--
UPN Suffixes	--
Anonymous Access (dsHeuristics)	Disabled

Table 1 - Forest Summary - SEVENKINGDOMS.LOCAL

1.1.1 Forest Diagram.



Active Directory Forest Architecture



Image preview: Opens the image in a new tab to view it at full resolution.

1.1.2 Certificate Authority

The following section provides a summary of the Active Directory PKI Infrastructure Information.

Certification Authority Root(s)

Name	Distinguished Name
SEVENKINGDOMS-CA	CN=SEVENKINGDOMS-CA,CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=sevenkingdoms,DC=local

Table 2 - Certificate Authority Root(s) - SEVENKINGDOMS.LOCAL

Certification Authority Issuer(s)

Name	DNS Name
SEVENKINGDOMS-CA	kingslanding.sevenkingdoms.local

Table 3 - Certificate Authority Issuer(s) - SEVENKINGDOMS.LOCAL

1.1.3 Optional Features

Name	Required Forest Mode	Enabled
Privileged Access Management Feature	Windows2016Forest	No
Recycle Bin Feature	Windows2008R2Forest	No

Table 4 - Optional Features - SEVENKINGDOMS.LOCAL

1.1.4 Replication

Replication is the process of transferring and updating Active Directory objects between domain controllers in the Active Directory domain and forest. The following section details Active Directory replication and its relationships.

1.1.4.1 Sites

Site Name	Description	Subnets	Domain Controllers
Default-First-Site-Name	--	No subnet assigned	KINGSLANDING WINTERFELL

Table 5 - Sites - SEVENKINGDOMS.LOCAL

Health Check:

Corrective Actions: Ensure Sites have an associated subnet. If subnets are not associated with AD Sites users in the AD Sites might choose a remote domain controller for authentication which in turn might result in excessive use of a remote domain controller.

Best Practice: It is a general rule of good practice to establish well-defined descriptions. This helps to speed up the fault identification process, as well as enabling better documentation of the environment.

Connection Objects

Name	From Server	To Server	From Site
<automatically generated>	KINGSLANDING	WINTERFELL	Default-First-Site-Name
<automatically generated>	WINTERFELL	KINGSLANDING	Default-First-Site-Name

Table 6 - Connection Objects - SEVENKINGDOMS.LOCAL

1.1.4.2 Site Inventory Diagram.

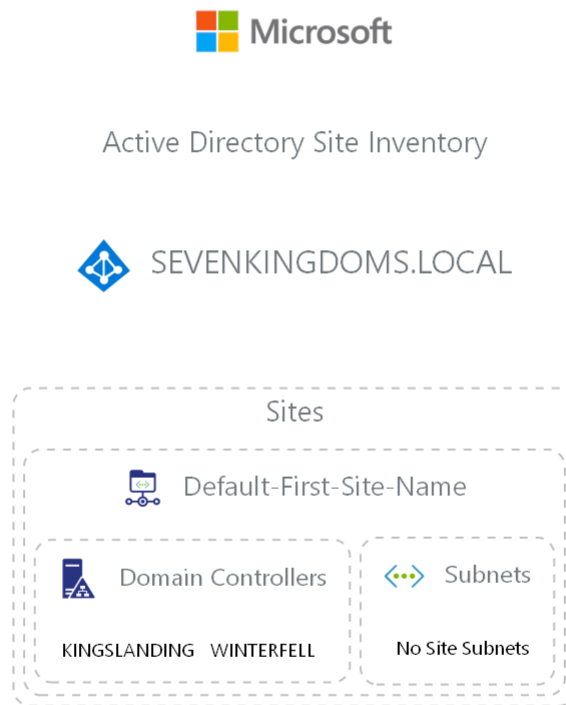


Image preview: Opens the image in a new tab to view it at full resolution.

1.1.4.3 Inter-Site Transports

Site links in Active Directory represent the inter-site connectivity and method used to transfer replication traffic. There are two transport protocols that can be used for replication via site links. The default protocol used in site link is IP, and it performs synchronous replication between available domain controllers. The SMTP method can be used when the link between sites is not reliable.

Name	Bridge All Site Links	Ignore Schedules
IP	Yes	No
SMTP	Yes	Yes

Table 7 - Inter-Site Transports - SEVENKINGDOMS.LOCAL

1.1.4.3.1 IP

1.1.4.3.1.1 Site Links

Site Link Name	DEFAULTIPSITELINK
Cost	100
Replication Frequency	180 min
Transport Protocol	IP
Options	Change Notification is Disabled
Sites	Default-First-Site-Name
Protected From Accidental Deletion	No
Description	--

Table 8 - Site Links - DEFAULTIPSITELINK

Health Check:

Best Practice: It is a general rule of good practice to establish well-defined descriptions. This helps to speed up the fault identification process, as well as enabling better documentation of the environment.

Best Practice: Enabling change notification treats an INTER-site replication connection like an INTRA-site connection. Replication between sites with change notification is almost instant. Microsoft recommends using an Option number value of 5 (Change Notification is Enabled without Compression).

Best Practice: If the Site Links in your Active Directory are not protected from accidental deletion, your environment can experience disruptions that might be caused by accidental bulk deletion of objects.

1.1.4.4 Sysvol Replication

DC Name	Replication Status	Domain
winterfell	Normal	north.sevenkingdoms.local
kingslanding	Normal	sevenkingdoms.local

Table 9 - Sysvol Replication - SEVENKINGDOMS.LOCAL

2 AD Domain Configuration

The following section provides a summary of the Active Directory Domain Information.

2.1 SEVENKINGDOMS.LOCAL

Microsoft Active Directory As Built Report - v1.0

The following section provides a summary of the Active Directory Domain Information.

Domain Name	sevenkingdoms
NetBIOS Name	SEVENKINGDOMS
Domain SID	S-1-5-21-3982372283-2816966531-3878323536
Domain Functional Level	Windows2016Domain
Domains	--
Forest	sevenkingdoms.local
Parent Domain	--
Replica Directory Servers	kingslanding.sevenkingdoms.local
Child Domains	north.sevenkingdoms.local
Domain Path	sevenkingdoms.local/
Computers Container	CN=Computers,DC=sevenkingdoms,DC=local
Domain Controllers Container	OU=Domain Controllers,DC=sevenkingdoms,DC=local
Systems Container	CN=System,DC=sevenkingdoms,DC=local
Users Container	CN=Users,DC=sevenkingdoms,DC=local
Deleted Objects Container	CN=Deleted Objects,DC=sevenkingdoms,DC=local
Foreign Security Principals Container	CN=ForeignSecurityPrincipals,DC=sevenkingdoms,DC=local
Lost And Found Container	CN=LostAndFound,DC=sevenkingdoms,DC=local
Quotas Container	CN=NTDS Quotas,DC=sevenkingdoms,DC=local
ReadOnly Replica Directory Servers	--
ms-DS-MachineAccountQuota	10
RID Issued/Available	1601 / 1073740222 (1% Issued)

Table 10 - Domain Summary - SEVENKINGDOMS.LOCAL

2.1.1 FSMO Roles

Infrastructure Master	kingslanding.sevenkingdoms.local
RID Master	kingslanding.sevenkingdoms.local
PDC Emulator Name	kingslanding.sevenkingdoms.local
Domain Naming Master	kingslanding.sevenkingdoms.local
Schema Master	kingslanding.sevenkingdoms.local

Table 11 - FSMO Roles - sevenkingdoms.local

Health Check:

Best Practice: The infrastructure master role in the domain SEVENKINGDOMS.LOCAL should be held by a domain controller that is not a global catalog server. This issue does not affect forests that have a single domain.

Reference: <http://go.microsoft.com/fwlink/?LinkId=168841>

2.1.2 Domain and Trusts

north.sevenkingdoms.local

Name	north.sevenkingdoms.local
Path	sevenkingdoms.local/System/north.sevenkingdoms.local
Source	sevenkingdoms
Target	north.sevenkingdoms.local
Trust Type	Uplevel
Trust Attributes	Intra-Forest Trust (trust within the forest)
Trust Direction	Bidirectional (two-way trust)
IntraForest	Yes
Selective Authentication	No
SID Filtering Forest Aware	No
SID Filtering Quarantined	No
TGT Delegation	No
Kerberos AES Encryption	No
Kerberos RC4 Encryption	No
Uplevel Only	No

Table 12 - Trusts - north.sevenkingdoms.local

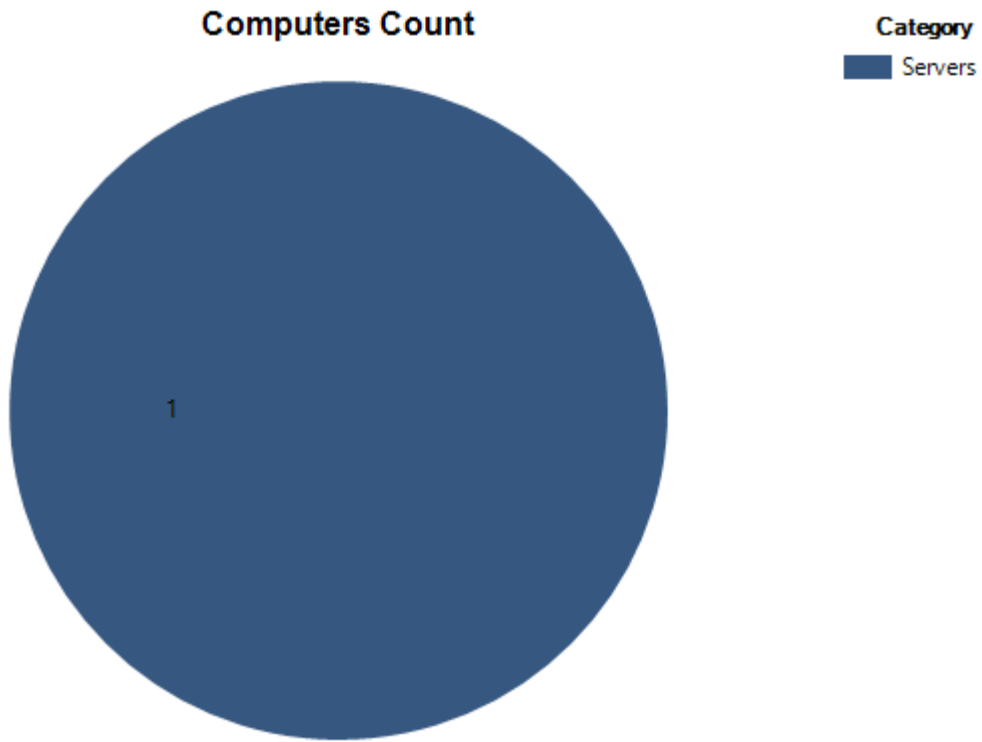
essos.local

Name	essos.local
Path	sevenkingdoms.local/System/essos.local
Source	sevenkingdoms
Target	essos.local
Trust Type	Uplevel
Trust Attributes	72
Trust Direction	Bidirectional (two-way trust)
IntraForest	No
Selective Authentication	No
SID Filtering Forest Aware	Yes
SID Filtering Quarantined	No
TGT Delegation	No
Kerberos AES Encryption	No
Kerberos RC4 Encryption	No
Uplevel Only	No

Table 13 - Trusts - essos.local

2.1.3 Domain Object Stats

Computers

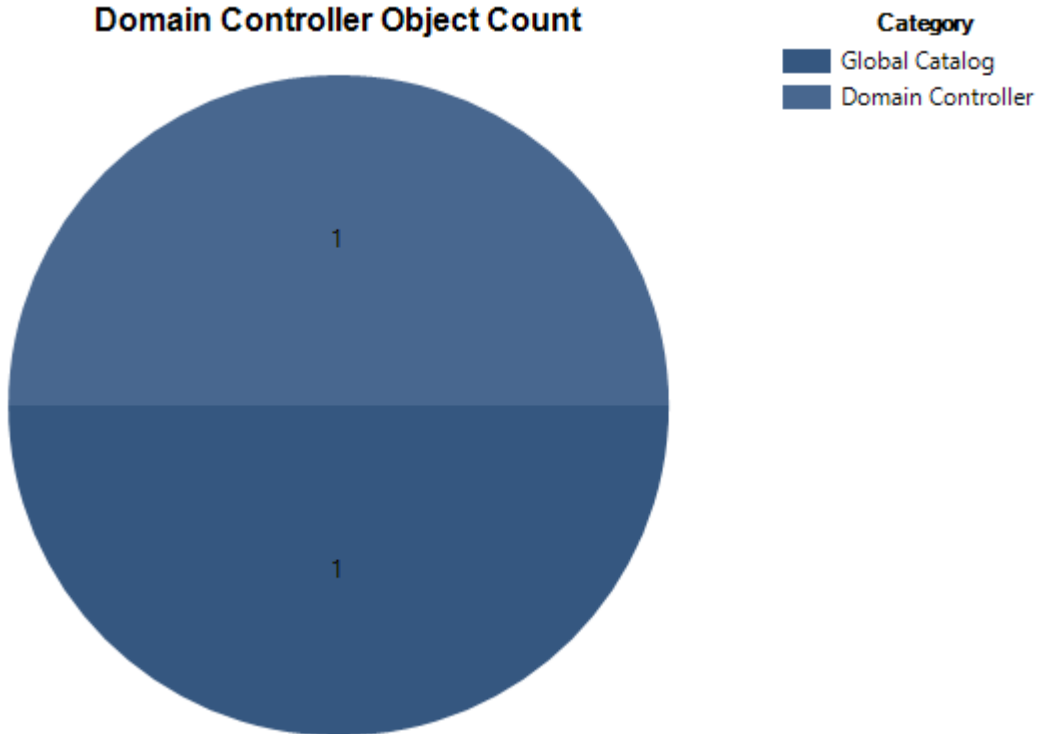


Computers	
Servers	1

Table 14 - Computers - SEVENKINGDOMS.LOCAL

Domain Controller

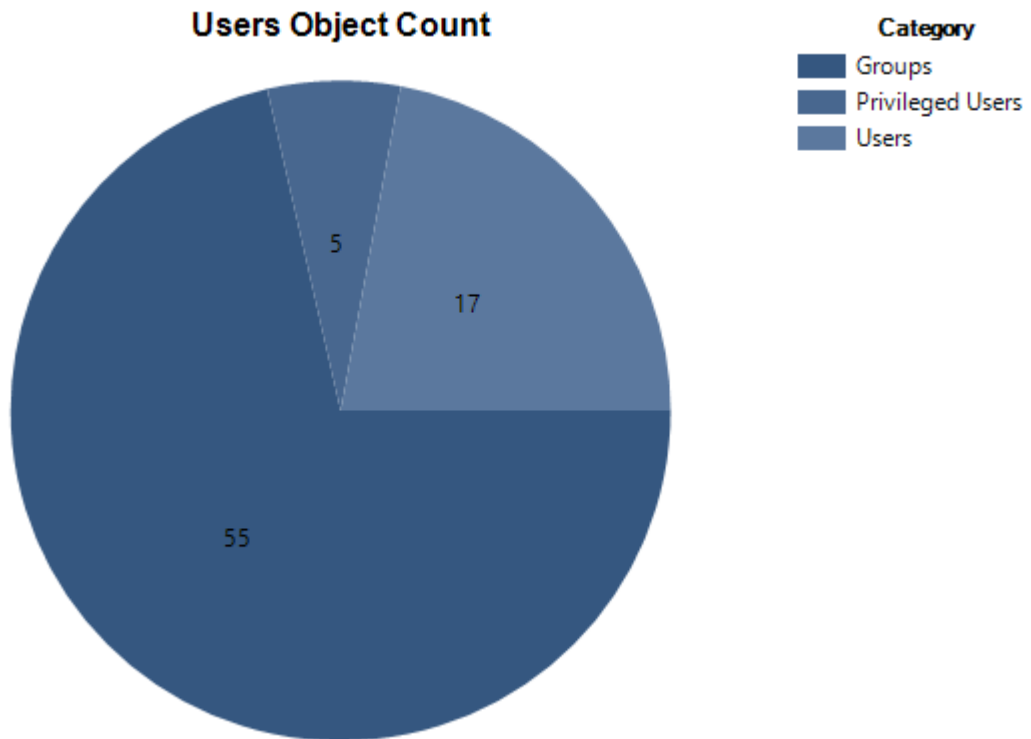
Domain Controller Object Count



Domain Controller	1
Global Catalog	1

Table 15 - Domain Controller - SEVENKINGDOMS.LOCAL

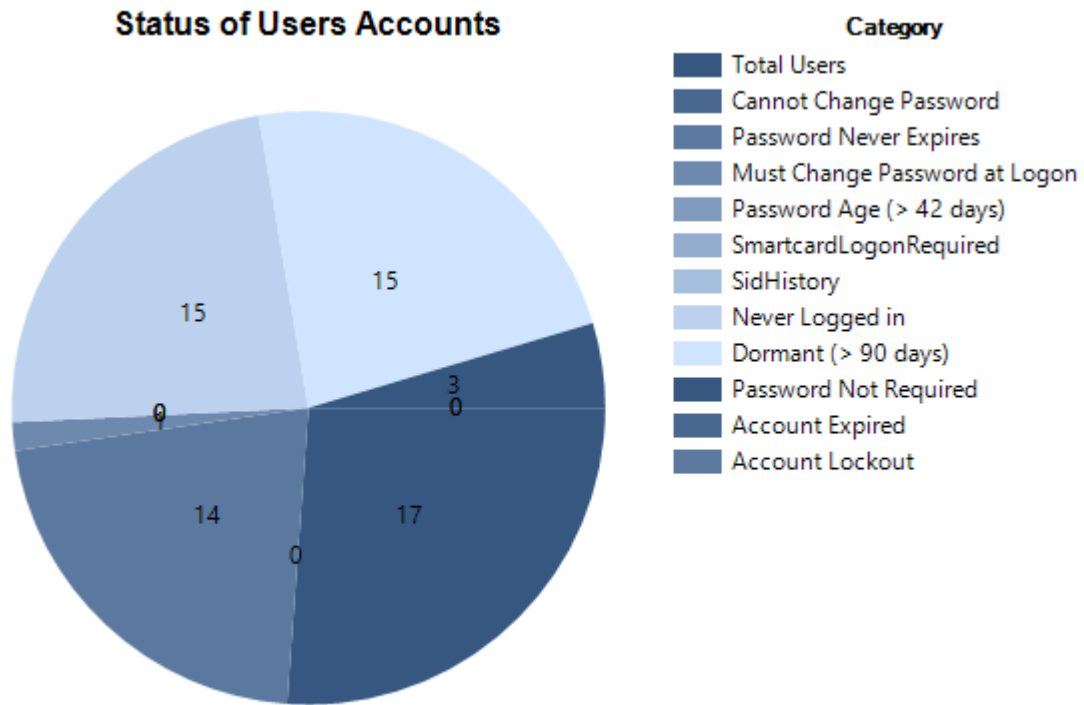
Users



Users	17
Privileged Users	5
Groups	55

Table 16 - User - SEVENKINGDOMS.LOCAL

2.1.4 Status of Users Accounts



Category	Enabled	Enabled %	Disabled	Disabled %	Total	Total %
Total Users	15	88.24	2	11.76	17	100
Cannot Change Password	1	5.88	1	5.88	0	0
Password Never Expires	13	76.47	1	5.88	14	82.35
Must Change Password at Logon	1	5.88	1	5.88	1	5.88
Password Age (> 42 days)	1	5.88	1	5.88	0	0
SmartcardLogonRequired	1	5.88	1	5.88	0	0
SidHistory	1	5.88	1	5.88	0	0
Never Logged in	13	76.47	2	11.76	15	88.24
Dormant (> 90 days)	13	76.47	2	11.76	15	88.24
Password Not Required	2	11.76	1	5.88	3	17.65
Account Expired	1	5.88	1	5.88	0	0
Account Lockout	1	5.88	1	5.88	0	0

Table 17 - Status of User Accounts - SEVENKINGDOMS.LOCAL

2.1.5 Privileged Groups

The following session details the members users within the privilege groups.

Domain Admins (3 Members)

Name	Last Logon Date	Password Never Expires	Account Enabled
Administrator	4/12/2024	**Yes	Yes
cersei.lannister	--	**Yes	Yes
robert.baratheon	--	**Yes	Yes

Table 18 - Domain Admins - SEVENKINGDOMS.LOCAL

Health Check:

Security Best Practice:

**Ensure there aren't any account with weak security posture.

Enterprise Admins (1 Members)

Name	Last Logon Date	Password Never Expires	Account Enabled
Administrator	4/12/2024	**Yes	Yes

Table 19 - Enterprise Admins - SEVENKINGDOMS.LOCAL

Health Check:

Security Best Practice:

Unless an account is doing specific tasks needing those highly elevated permissions, every account should be removed from Enterprise Admins (EA) group. A side benefit of having an empty Enterprise Admins group is that it adds just enough friction to ensure that enterprise-wide changes requiring Enterprise Admin rights are done purposefully and methodically.

**Ensure there aren't any account with weak security posture.

Administrators (4 Members)

Name	Last Logon Date	Password Never Expires	Account Enabled
Administrator	4/12/2024	**Yes	Yes
cersei.lannister	--	**Yes	Yes
robert.baratheon	--	**Yes	Yes
vagrant	4/12/2024	**Yes	Yes

Table 20 - Administrators - SEVENKINGDOMS.LOCAL

Health Check:

Security Best Practice:

**Ensure there aren't any account with weak security posture.

Remote Desktop Users (8 Members)

Name	Last Logon Date	Password Never Expires	Account Enabled
cersei.lannister	--	**Yes	Yes
joffrey.baratheon	--	**Yes	Yes
lord.varys	--	**Yes	Yes
maester.pycelle	--	**Yes	Yes
petyer.baelish	--	**Yes	Yes
renly.baratheon	--	**Yes	Yes
robert.baratheon	--	**Yes	Yes
stannis.baratheon	--	**Yes	Yes

Table 21 - Remote Desktop Users - SEVENKINGDOMS.LOCAL

Health Check:

Security Best Practice:

**Ensure there aren't any account with weak security posture.

Schema Admins (1 Members)

Name	Last Logon Date	Password Never Expires	Account Enabled
Administrator	4/12/2024	**Yes	Yes

Table 22 - Schema Admins - SEVENKINGDOMS.LOCAL

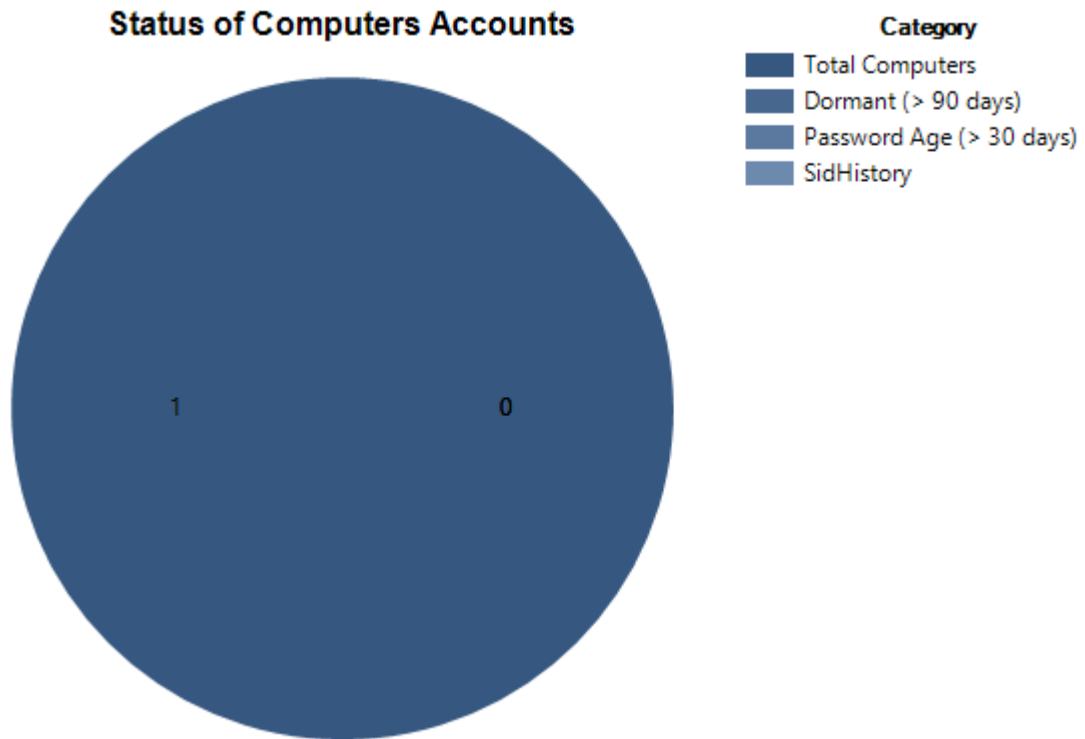
Health Check:

Security Best Practice:

The Schema Admins group is a privileged group in a forest root domain. Members of the Schema Admins group can make changes to the schema, which is the framework for the Active Directory forest. Changes to the schema are not frequently required. This group only contains the Built-in Administrator account by default. Additional accounts must only be added when changes to the schema are necessary and then must be removed.

**Ensure there aren't any account with weak security posture.

2.1.6 Status of Computer Accounts



Category	Enabled	Enabled %	Disabled	Disabled %	Total	Total %
Total Computers	1	0	1	0	1	0
Dormant (> 90 days)	1	0	1	0	0	0
Password Age (> 30 days)	1	0	1	0	0	0
SidHistory	1	0	1	0	0	0

Table 23 - Status of Computer Accounts - SEVENKINGDOMS.LOCAL

2.1.7 Operating Systems Count

Operating System	Count
Windows Server 2019 Datacenter Evaluation	1

Table 24 - Operating System Count - SEVENKINGDOMS.LOCAL

2.1.8 Default Domain Password Policy

Password Must Meet Complexity Requirements	No
Path	sevenkingdoms.local/
Lockout Duration	05 minutes

Lockout Threshold	5
Lockout Observation Window	05 minutes
Max Password Age	37201 days
Min Password Age	01 days
Min Password Length	5
Enforce Password History	24
Store Password using Reversible Encryption	No

Table 25 - Default Domain Password Policy - SEVENKINGDOMS.LOCAL

2.1.9 Windows LAPS

Name	
Domain Name	sevenkingdoms.local
Enabled	No
Distinguished Name	

Table 26 - Windows LAPS - SEVENKINGDOMS.LOCAL

Health Check:

Security Best Practice: LAPS simplifies password management while helping customers implement additional recommended defenses against cyberattacks. In particular, the solution mitigates the risk of lateral escalation that results when customers use the same administrative local account and password combination on their computers. Download, install, and configure Microsoft LAPS or a third-party solution.

2.1.10 Foreign Security Principals

Name	Principal Name
NT AUTHORITY\INTERACTIVE	Users
NT AUTHORITY\Authenticated Users	Pre-Windows 2000 Compatible Access Certificate Service DCOM Access Users
NT AUTHORITY\IUSR	--
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Windows Authorization Access Group
ESSOS\daenerys.targaryen	AcrossTheNarrowSea

Table 27 - Foreign Security Principals - SEVENKINGDOMS.LOCAL

2.1.11 Health Checks

Naming Context Last Backup

The following section details naming context last backup time for Domain SEVENKINGDOMS.LOCAL.

Naming Context	Last Backup	Last Backup in Days
CN=Configuration,DC=sevenkingdoms,DC=local	2024:04:12	0
CN=Schema,CN=Configuration,DC=sevenkingdoms,DC=local	2024:04:12	0
DC=DomainDnsZones,DC=sevenkingdoms,DC=local	2024:04:12	0
DC=ForestDnsZones,DC=sevenkingdoms,DC=local	2024:04:12	0
DC=sevenkingdoms,DC=local	2024:04:12	0

Table 28 - Naming Context Last Backup - SEVENKINGDOMS.LOCAL

Sysvol Replication Status

The following section details the sysvol folder replication status for Domain SEVENKINGDOMS.LOCAL.

DC Name	Replication Status	GPO Count	Sysvol Count	Identical Count	Stop Replication On AutoRecovery
KINGSLANDING	Unknown	2	0	No	--

Table 29 - Sysvol Replication Status - SEVENKINGDOMS.LOCAL

Health Check:

Corrective Actions: SYSVOL is a special directory that resides on each domain controller (DC) within a domain. The directory comprises folders that store Group Policy objects (GPOs) and log on scripts that clients need to access and synchronize between DCs. For these logon scripts and GPOs to function properly, SYSVOL should be replicated accurately and rapidly throughout the domain. Ensure that proper SYSVOL replication is in place to ensure identical GPO/SYSVOL content for the domain controller across all Active Directory domains.

Sysvol Content Status

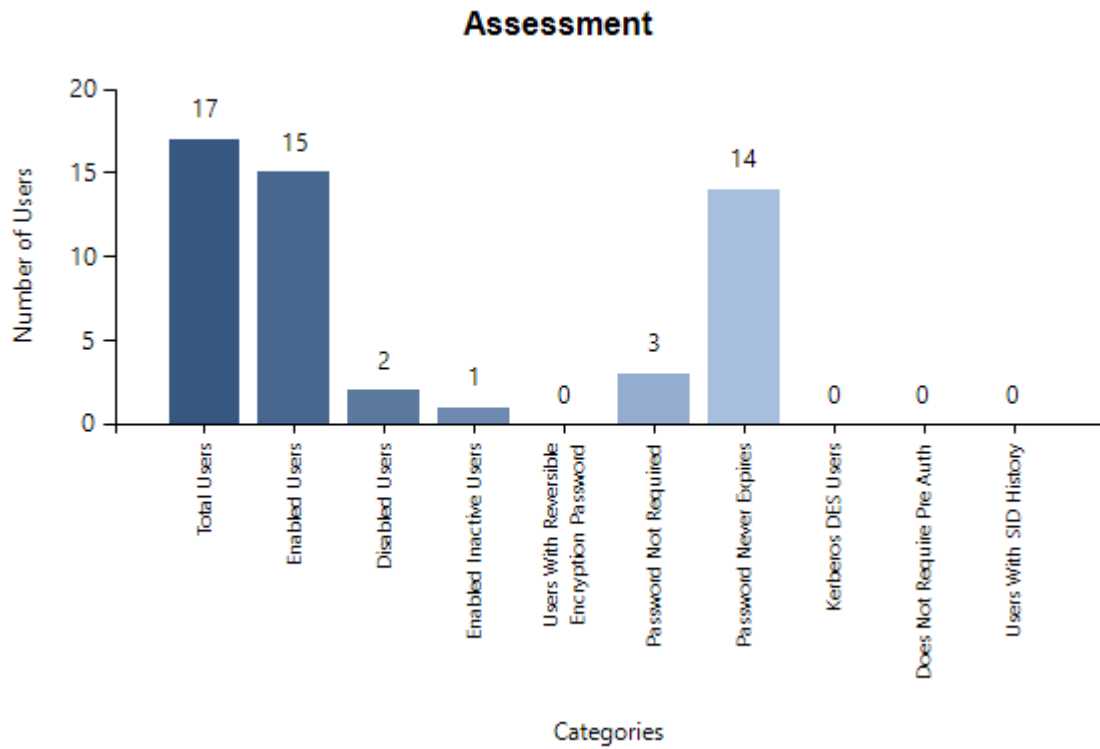
The following section details domain SEVENKINGDOMS.LOCAL sysvol health status.

Extension	File Count	Size
.inf	2	0.01 MB
.INI	2	0.00 MB
.pol	1	0.00 MB

Table 30 - Sysvol Content Status - SEVENKINGDOMS.LOCAL

Account Security Assessment

The following section provide a summary of the Account Security Assessment on Domain SEVENKINGDOMS.LOCAL.



Total Users	17
Enabled Users	15
Disabled Users	2
Enabled Inactive Users	1
Users With Reversible Encryption Password	0
Password Not Required	3
Password Never Expires	14
Kerberos DES Users	0
Does Not Require Pre Auth	0
Users With SID History	0

Table 31 - Account Security Assessment - SEVENKINGDOMS.LOCAL

Health Check:

Corrective Actions: Ensure there aren't any account with weak security posture.

Privileged Users Assessment

The following section details probable AD Admin accounts (user accounts with AdminCount set to 1) on Domain SEVENKINGDOMS.LOCAL

Username	Password Last Set	Last Logon Date	Email Enabled?	Trusted for Delegation
Administrator	4/12/2024	4/12/2024	No	** Yes
vagrant	5/12/2021	4/12/2024	No	** Yes
krbtgt	4/12/2024	--	No	** Yes
cersei.lannister	4/12/2024	--	No	** Yes
robert.baratheon	4/12/2024	--	No	** Yes

Table 32 - Privileged User Assessment - SEVENKINGDOMS.LOCAL

Health Check:

Security Best Practice:

** Privileged accounts such as those belonging to any of the administrator groups must not be trusted for delegation. Allowing privileged accounts to be trusted for delegation provides a means for privilege escalation from a compromised system. Delegation of privileged accounts must be prohibited. Reference: https://www.stigviewer.com/stig/active_directory_domain/2017-12-15/finding/V-36435

Service Accounts Assessment

The following section details probable AD Service Accounts (user accounts with SPNs) on Domain SEVENKINGDOMS.LOCAL

Username	Enabled	Password Last Set	Last Logon Date	Service Principal Name
krbtgt	No	4/12/2024	--	kadmin/changepw

Table 33 - Service Accounts Assessment - SEVENKINGDOMS.LOCAL

Health Check:

KRBTGT Account Audit

The following section provide a summary of KRBTGT account on Domain SEVENKINGDOMS.LOCAL.

Name	krbtgt
Created	04/12/2024 13:47:36
Password Last Set	04/12/2024 13:47:36
Distinguished Name	CN=krbtgt,CN=Users,DC=sevenkingdoms,DC=local

Table 34 - KRBTGT Account Audit - SEVENKINGDOMS.LOCAL

Health Check:

Best Practice: Microsoft advises changing the krbtgt account password at regular intervals to keep the environment more secure.

Administrator Account Audit

The following section provide a summary of Administrator account on Domain SEVENKINGDOMS.LOCAL.

Name	Administrator
Created	04/12/2024 13:43:04
Password Last Set	04/12/2024 13:35:58
Last Logon Date	04/12/2024 13:57:29
Distinguished Name	CN=Administrator,CN=Users,DC=sevenkingdoms,DC=local

Table 35 - Administrator Account Audit - SEVENKINGDOMS.LOCAL

Health Check:

Best Practice: Microsoft advises changing the administrator account password at regular intervals to keep the environment more secure.

2.1.12 Domain Controllers

The following section provides detailed information about Active Directory domain controllers.

2.1.12.1 KINGSLANDING

General Information

DC Name	kingslanding.sevenkingdoms.local
Domain Name	sevenkingdoms.local
Site	Default-First-Site-Name
Global Catalog	Yes
Read Only	No
Location	
Computer Object SID	S-1-5-21-3982372283-2816966531-3878323536-1001
Operating System	Windows Server 2019 Datacenter Evaluation
Description	

Table 36 - General Information - KINGSLANDING

Partitions

Default Partition	DC=sevenkingdoms,DC=local
Partitions	DC=ForestDnsZones,DC=sevenkingdoms,DC=local DC=DomainDnsZones,DC=sevenkingdoms,DC=local

	CN=Schema,CN=Configuration,DC=sevenkingdoms,DC=local
	CN=Configuration,DC=sevenkingdoms,DC=local
	DC=sevenkingdoms,DC=local
	DC=north,DC=sevenkingdoms,DC=local

Table 37 - Partitions - KINGSLANDING

Networking Settings

IPv4 Addresses	--
IPv6 Addresses	--
LDAP Port	389
SSL Port	636

Table 38 - Networking Settings - KINGSLANDING

Hardware Inventory

Name	KINGSLANDING
Windows Product Name	Windows Server 2019 Datacenter Evaluation
Windows Build Number	10.0.17763
AD Domain	sevenkingdoms.local
Windows Installation Date	04/12/2024 10:56:06
Time Zone	(UTC-08:00) Pacific Time (US & Canada)
License Type	Retail:TB:Eval
Partial Product Key	H6F8M
Manufacturer	VMware, Inc.
Model	VMware Virtual Platform
Processor Model	Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz
Number of Processors	4
Number of CPU Cores	1
Number of Logical Cores	1
Physical Memory	5.86 GB

Table 39 - Hardware Inventory - KINGSLANDING

Health Check:

Best Practice: Microsoft recommend putting enough RAM 8GB+ to load the entire DIT into memory, plus accommodate the operating system and other installed applications, such as anti-virus, backup software, monitoring, and so on.

2.1.12.2 DNS IP Configuration

DC Name	Interface	Preferred DNS	Alternate DNS	DNS 3	DNS 4
KINGSLANDING	Ethernet0	127.0.0.1	--	--	--

DC Name	Interface	Preferred DNS	Alternate DNS	DNS 3	DNS 4
KINGSLANDING	Ethernet1	127.0.0.1	--	--	--

Table 40 - DNS IP Configuration - SEVENKINGDOMS.LOCAL

Health Check:

Best Practices: DNS configuration on network adapter should include the loopback address, but not as the first entry.

Best Practices: For redundancy reasons, the DNS configuration on the network adapter should include an Alternate DNS address.

2.1.12.3 NTDS Information

DC Name	Database File	Database Size	Log Path	SysVol Path
KINGSLANDING	C:\Windows\NTDS\ntds.dit	18.00 MB	C:\Windows\NTDS	C:\Windows\SYSVOL\sysvol

Table 41 - NTDS Database File Usage - SEVENKINGDOMS.LOCAL

2.1.12.4 Time Source Information

Name	Time Server	Type
KINGSLANDING	Domain Hierarchy	DOMHIER

Table 42 - Time Source Configuration - SEVENKINGDOMS.LOCAL

2.1.12.5 SRV Records Status

Name	A Record	KDC SRV	PDC SRV	GC SRV	DC SRV
KINGSLANDING	OK	OK	OK	OK	OK

Table 43 - SRV Records Status - SEVENKINGDOMS.LOCAL

2.1.12.6 File Shares

The following domain controllers have non-default file shares.

KINGSLANDING

Name	Path	Description
CertEnroll	C:\Windows\system32\CertSrv\CertEnroll	Active Directory Certificate Services share

Table 44 - File Shares - KINGSLANDING

Health Check:

Best Practice: Only netlogon, sysvol and the default administrative shares should exist on a Domain Controller. If possible, non default file shares should be moved to another server, preferably a dedicated file server.

2.1.12.7 Roles

The following section provides a summary of installed role & features on sevenkingdoms.local DCs.

KINGSLANDING

Name	Parent	Description
Active Directory Certificate Services	Role	Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.
Active Directory Domain Services	Role	Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
DNS Server	Role	Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.
File and Storage Services	Role	File and Storage Services includes services that are always installed, as well as functionality that you can install to help manage file servers and storage.
Web Server (IIS)	Role	Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Table 45 - Roles - KINGSLANDING

Health Check:

Best Practices: Domain Controllers should have limited software and agents installed including roles and services. Non-essential code running on Domain Controllers is a risk to the enterprise Active Directory environment. A Domain Controller should only run required software, services and roles critical to essential operation.

2.1.12.8 DC Diagnostic

The following section provides a summary of the Active Directory DC Diagnostic.

KINGSLANDING

Microsoft Active Directory As Built Report - v1.0

Test Name	Result	Impact	Description
Replications	Passed	High	Makes a deep validation to check the main replication for all naming contexts in this Domain Controller.
RidManager	Passed	High	Validates this Domain Controller can locate and contact the RID Master FSMO role holder. This test is skipped in RODCs.
ObjectsReplicated	Passed	High	Checks the replication health of core objects and attributes.
NCSecDesc	Passed	Medium	Validates if permissions are correctly set in this Domain Controller for all naming contexts. Those permissions directly affect replications health.
NetLogons	Passed	High	Validates if core security groups (including administrators and Authenticated Users) can connect and read NETLOGON and SYSVOL folders. It also validates access to IPC\$. which can lead to failures in organizations that disable IPC\$.
Services	Passed	High	Validates if the core Active Directory services are running in this Domain Controller. The services verified are: RPCSS, EVENTSYSTEM, DNSCACHE, ISMSERV, KDC, SAMSS, WORKSTATION, W32TIME, NETLOGON, NTDS (in case Windows Server 2008 or newer) and DFSR (if SYSVOL is using DFSR).
VerifyReplicas	Passed	High	Checks that all application directory partitions are fully instantiated on all replica servers.
DNS	Passed	Medium	DNS Includes six optional DNS-related tests, as well as the Connectivity test, which runs by default.
VerifyReferences	Passed	High	Validates that several attributes are present for the domain in the container and subcontainers in the DC objects. This test will fail if any attribute is missing.
SystemLog	Failed	Low	Checks if there is any errors in the Event Viewer > System event log in the past 60 minutes. Since the System event log records data from many places, errors reported here may lead to false positive and must be investigated further. The impact of this validation is marked as Low.
Topology	Passed	Medium	Topology Checks that the KCC has generated a fully connected topology for all domain controllers.
CutoffServers	Passed	Medium	Checks for any server that is not receiving replications because its partners are not running
FrsEvent	Passed	Medium	Checks if theres any errors in the event logs regarding FRS replication. If running Windows Server 2008 R2 or newer on all Domain Controllers is possible SYSVOL were already migrated to DFSR, in this case errors found here can be ignored.
CheckSecurityError	Passed	Medium	Reports on the overall health of replication with respect to Active Directory security in domain controllers running Windows Server 2003 SP1.

Microsoft Active Directory As Built Report - v1.0

Test Name	Result	Impact	Description
Connectivity	Passed	Medium	Initial connection validation, checks if the DC can be located in the DNS, validates the ICMP ping (1 hop), checks LDAP binding and also the RPC connection. This initial test requires ICMP, LDAP, DNS and RPC connectivity to work properly.
Advertising	Passed	High	Validates this Domain Controller can be correctly located through the KDC service. It does not validate the Kerberos tickets answer or the communication through the TCP and UDP port 88.
DFSREvent	Failed	Medium	Checks if theres any errors in the event logs regarding DFSR replication. If running Windows Server 2008 or older on all Domain Controllers is possible SYSVOL is still using FRS, and in this case errors found here can be ignored. Obs. is highly recommended to migrate SYSVOL to DFSR.
KnowsOfRoleHolders	Passed	High	Checks if this Domain Controller is aware of which DC (or DCs) hold the FSMOs.
MachineAccount	Passed	High	Checks if this computer account exist in Active Directory and the main attributes are set. If this validation reports error. the following parameters of DCDIAG might help: /RecreateMachineAccount and /FixMachineAccount.
KccEvent	Passed	High	Validates through KCC there were no errors in the Event Viewer > Applications and Services Logs > Directory Services event log in the past 15 minutes (default time).
SysVolCheck	Passed	High	Validates if the registry key HKEY_Local_Machine\System\CurrentControlSet\Services\Netlogon\Parameters\SysvolReady=1 exist. This registry has to exist with value 1 for the DCs SYSVOL to be advertised.
FrsSysVol	Passed	Medium	Checks that the file replication system (FRS) system volume (SYSVOL) is ready

Table 46 - DCdiag Test Status - KINGSLANDING

2.1.12.9 Infrastructure Services

The following section provides a summary of the Domain Controller Infrastructure services status.

KINGSLANDING

Display Name	Short Name	Status
Active Directory Certificate Services	CertSvc	Running
Active Directory Domain Services	NTDS	Running
Active Directory Web Services	ADWS	Running
COM+ Event System	EVENTSYSTEM	Running

Microsoft Active Directory As Built Report - v1.0

Display Name	Short Name	Status
DFS Replication	DFSR	Running
DNS Client	DNSCACHE	Running
DNS Server	DNS	Running
Intersite Messaging	IsmServ	Running
Kerberos Key Distribution Center	Kdc	Running
NetLogon	Netlogon	Running
Print Spooler	Spooler	Running
Remote Procedure Call (RPC)	RPCSS	Running
Security Accounts Manager	SAMSS	Running
Windows Time	W32Time	Running
WORKSTATION	LanmanWorkstation	Running

Table 47 - Infrastructure Services Status - KINGSLANDING

Health Check:

Corrective Actions: Disable Print Spooler service on DCs and all servers that do not perform Print services.

2.1.13 Replication Connection

The following section provides detailed information about Replication Connection.

Site: Default-First-Site-Name: From: WINTERFELL To: KINGSLANDING

Name	<automatically generated>
From Site	Default-First-Site-Name
GUID	11bfc0d6-1d25-4dec-b4c7-85a51ad011d5
Description	--
From Server	WINTERFELL
To Server	KINGSLANDING
Replicated Naming Contexts	DC=ForestDnsZones,DC=sevenkingdoms,DC=local DC=DomainDnsZones,DC=sevenkingdoms,DC=local CN=Schema,CN=Configuration,DC=sevenkingdoms,DC=local CN=Configuration,DC=sevenkingdoms,DC=local DC=sevenkingdoms,DC=local
Transport Protocol	
Auto Generated	Yes
Enabled	Yes
Created	Fri, 12 Apr 2024 17:58:32 GMT

Table 48 - Replication Connection - KINGSLANDING

2.1.14 Replication Status

From Server	To Server	From Site	Last Success Time	Last Failure Status	Last Failure Time	Failures
WINTERFELL	KINGSLANDI NG	Default-First- Site-Name	2024-04-12 22:15:52	0	0	0
WINTERFELL	KINGSLANDI NG	Default-First- Site-Name	2024-04-12 22:16:24	0	0	0
WINTERFELL	KINGSLANDI NG	Default-First- Site-Name	2024-04-12 22:15:52	0	0	0
WINTERFELL	KINGSLANDI NG	Default-First- Site-Name	2024-04-12 22:15:52	0	0	0

Table 49 - Replication Status - SEVENKINGDOMS.LOCAL

2.1.15 Group Policy Objects

The following section provides a summary of the Group Policy Objects for domain SEVENKINGDOMS.LOCAL.

Default Domain Policy

GPO Status	All Settings Enabled
GUID	31b2f340-016d-11d2-945f-00c04fb984f9
Created	04/12/2024
Modified	04/12/2024
Owner	SEVENKINGDOMS\Domain Admins
Computer Version	4 (AD), 4 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	sevenkingdoms.local
Description	--

Table 50 - GPO - Default Domain Policy

Default Domain Controllers Policy

GPO Status	All Settings Enabled
GUID	6ac1786c-016f-11d2-945f-00c04fb984f9
Created	04/12/2024
Modified	04/12/2024
Owner	SEVENKINGDOMS\Domain Admins
Computer Version	4 (AD), 4 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)

WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	sevenkingdoms.local/Domain Controllers
Description	--

Table 51 - GPO - Default Domain Controllers Policy

2.1.15.1 Central Store Repository

Domain	Configured	Central Store Path
SEVENKINGDOMS.LOCAL	No	\\sevenkingdoms.local\SYSVOL\sevenkingdoms.local\Policies\PolicyDefinitions

Table 52 - GPO Central Store - SEVENKINGDOMS.LOCAL

Health Check:

Best Practices: The group policy central store is a central location to store all the group policy template files. This eliminates the need for admins to load and open group policy template files on systems used to manage group policy. Ensure Central Store is deployed to centralized GPO repository.

2.1.16 Organizational Units

The following section provides a summary of Active Directory Organizational Unit information.

Name	Linked GPO	Protected
Crownlands	--	Yes
Domain Controllers	Default Domain Controllers Policy	No
Dorne	--	Yes
IronIslands	--	Yes
Reach	--	Yes
Riverlands	--	Yes
Stormlands	--	Yes
Vale	--	Yes
Westerlands	--	Yes

Table 53 - Organizational Unit - SEVENKINGDOMS.LOCAL

Health Check:

Best Practice: If the Organizational Units in your Active Directory are not protected from accidental deletion, your environment can experience disruptions that might be caused by accidental bulk deletion of objects. All OUs in this domain should be protected from accidental deletion

2.2 NORTH.SEVENKINGDOMS.LOCAL

The following section provides a summary of the Active Directory Domain Information.

Domain Name	north
NetBIOS Name	NORTH
Domain SID	S-1-5-21-3784733952-806722479-2510178485
Domain Functional Level	Windows2016Domain
Domains	--
Forest	sevenkingdoms.local
Parent Domain	sevenkingdoms.local
Replica Directory Servers	winterfell.north.sevenkingdoms.local
Child Domains	--
Domain Path	north.sevenkingdoms.local/
Computers Container	CN=Computers,DC=north,DC=sevenkingdoms,DC=local
Domain Controllers Container	OU=Domain Controllers,DC=north,DC=sevenkingdoms,DC=local
Systems Container	CN=System,DC=north,DC=sevenkingdoms,DC=local
Users Container	CN=Users,DC=north,DC=sevenkingdoms,DC=local
Deleted Objects Container	CN=Deleted Objects,DC=north,DC=sevenkingdoms,DC=local
Foreign Security Principals Container	CN=ForeignSecurityPrincipals,DC=north,DC=sevenkingdoms,DC=local
Lost And Found Container	CN=LostAndFound,DC=north,DC=sevenkingdoms,DC=local
Quotas Container	CN=NTDS Quotas,DC=north,DC=sevenkingdoms,DC=local
ReadOnly Replica Directory Servers	--
ms-DS-MachineAccountQuota	10
RID Issued/Available	1601 / 1073740222 (1% Issued)

Table 54 - Domain Summary - NORTH.SEVENKINGDOMS.LOCAL

2.2.1 FSMO Roles

Infrastructure Master	winterfell.north.sevenkingdoms.local
RID Master	winterfell.north.sevenkingdoms.local
PDC Emulator Name	winterfell.north.sevenkingdoms.local
Domain Naming Master	kingslanding.sevenkingdoms.local
Schema Master	kingslanding.sevenkingdoms.local

Table 55 - FSMO Roles - north.sevenkingdoms.local

Health Check:

Best Practice: The infrastructure master role in the domain NORTH.SEVENKINGDOMS.LOCAL should be held by a domain controller that is not a global catalog server. This issue does not affect forests that have a single domain.

Reference: <http://go.microsoft.com/fwlink/?LinkId=168841>

2.2.2 Domain and Trusts

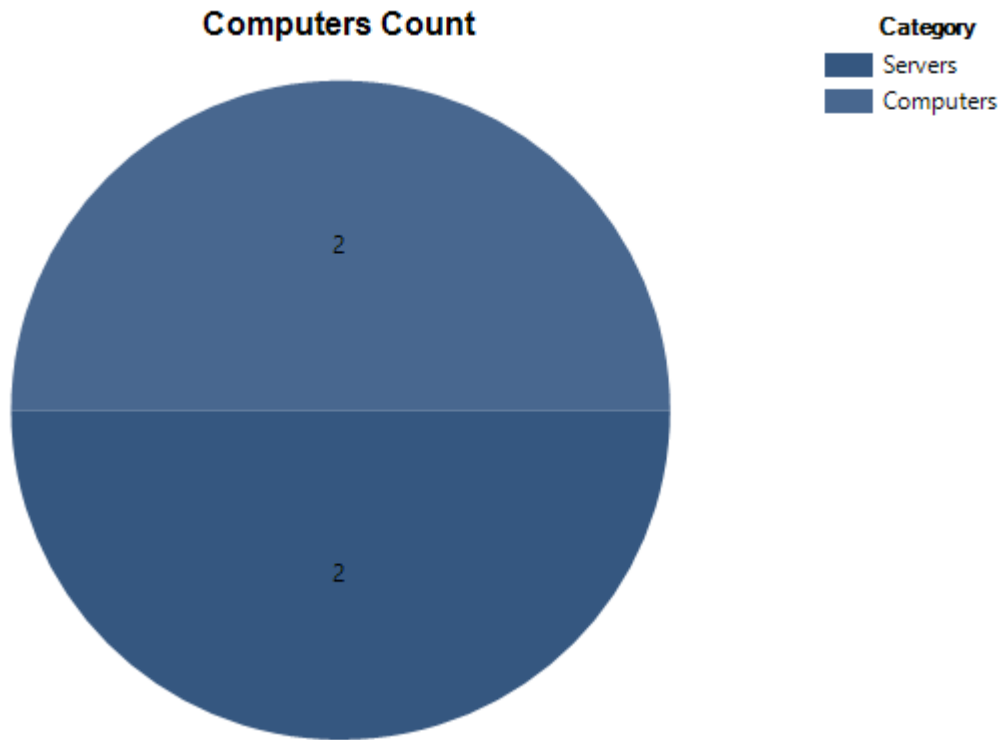
sevenkingdoms.local

Name	sevenkingdoms.local
Path	north.sevenkingdoms.local/System/sevenkingdoms.local
Source	north
Target	sevenkingdoms.local
Trust Type	Uplevel
Trust Attributes	Intra-Forest Trust (trust within the forest)
Trust Direction	Bidirectional (two-way trust)
IntraForest	Yes
Selective Authentication	No
SID Filtering Forest Aware	No
SID Filtering Quarantined	No
TGT Delegation	No
Kerberos AES Encryption	No
Kerberos RC4 Encryption	No
Uplevel Only	No

Table 56 - Trusts - sevenkingdoms.local

2.2.3 Domain Object Stats

Computers

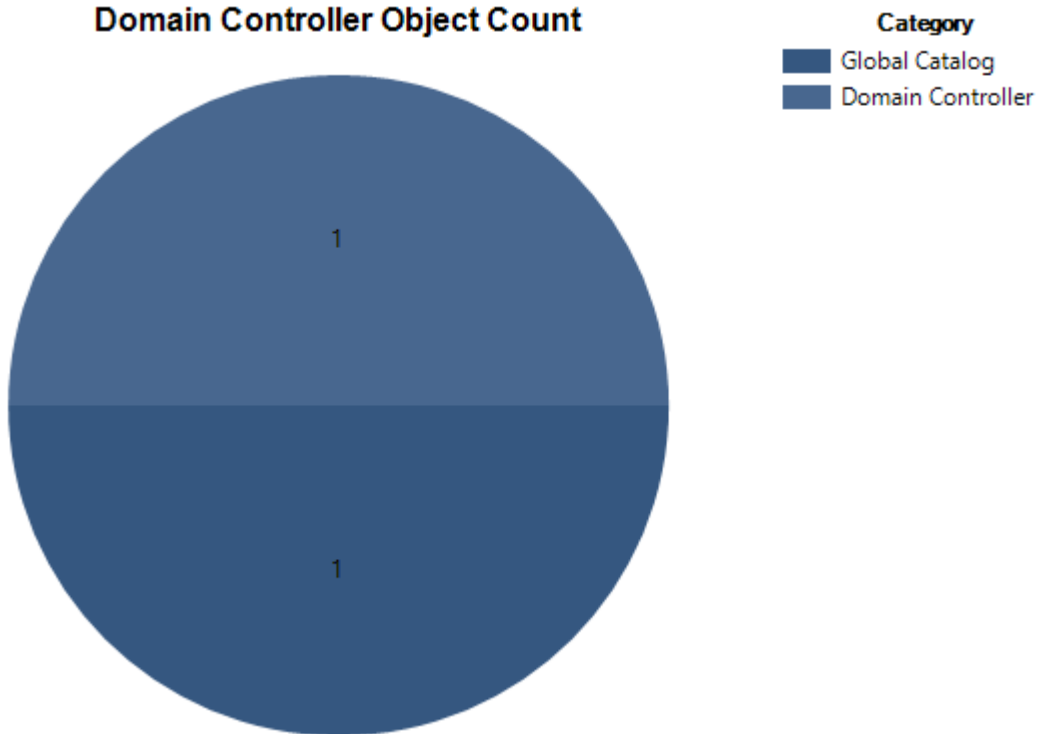


Computers	2
Servers	2

Table 57 - Computers - NORTH.SEVENKINGDOMS.LOCAL

Domain Controller

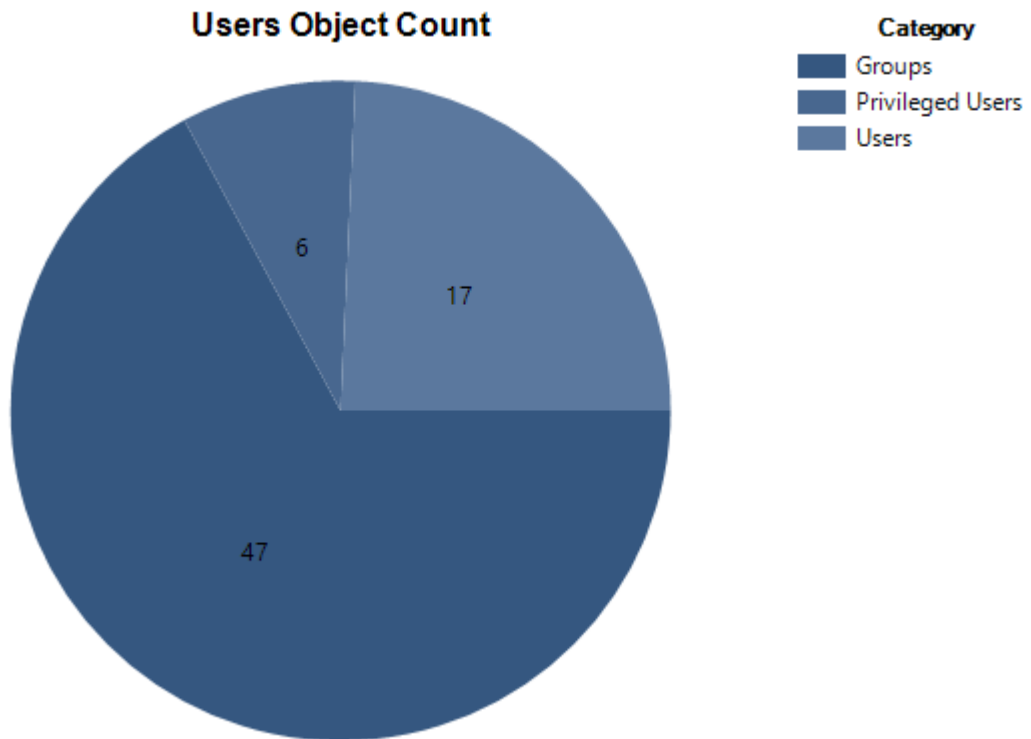
Domain Controller Object Count



Domain Controller	1
Global Catalog	1

Table 58 - Domain Controller - NORTH.SEVENKINGDOMS.LOCAL

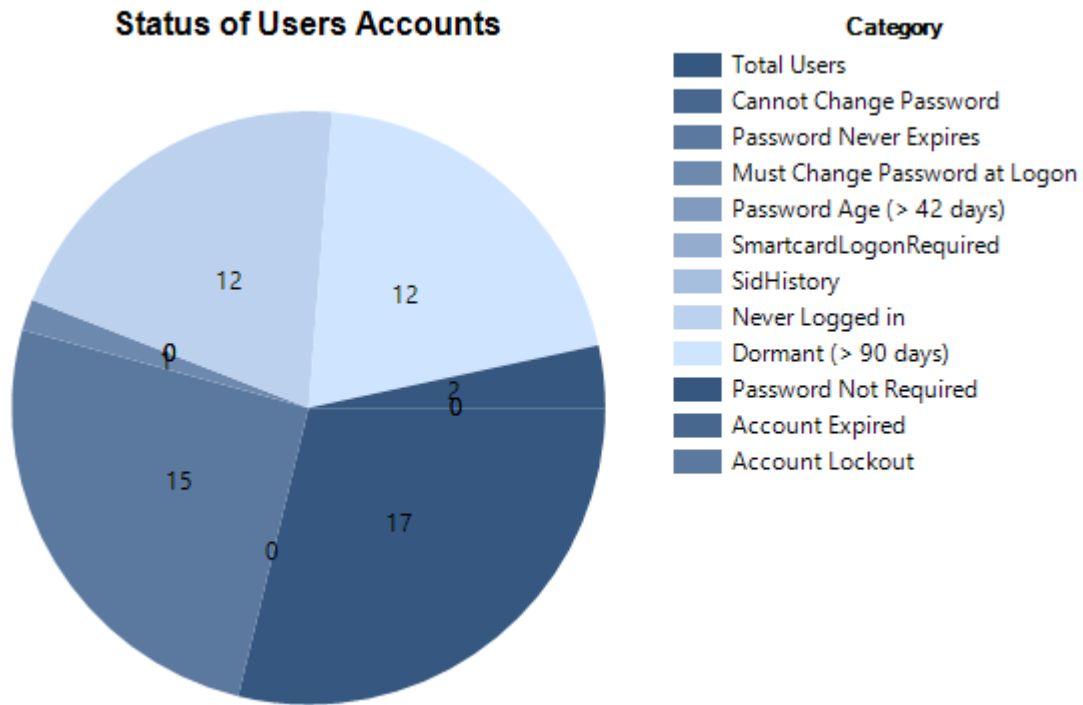
Users



Users	17
Privileged Users	6
Groups	47

Table 59 - User - NORTH.SEVENKINGDOMS.LOCAL

2.2.4 Status of Users Accounts



Category	Enabled	Enabled %	Disabled	Disabled %	Total	Total %
Total Users	15	88.24	2	11.76	17	100
Cannot Change Password	1	5.88	1	5.88	0	0
Password Never Expires	14	82.35	1	5.88	15	88.24
Must Change Password at Logon	1	5.88	1	5.88	1	5.88
Password Age (> 42 days)	1	5.88	1	5.88	0	0
SmartcardLogonRequired	1	5.88	1	5.88	0	0
SidHistory	1	5.88	1	5.88	0	0
Never Logged in	10	58.82	2	11.76	12	70.59
Dormant (> 90 days)	10	58.82	2	11.76	12	70.59
Password Not Required	1	5.88	1	5.88	2	11.76
Account Expired	1	5.88	1	5.88	0	0
Account Lockout	1	5.88	1	5.88	0	0

Table 60 - Status of User Accounts - NORTH.SEVENKINGDOMS.LOCAL

2.2.5 Privileged Groups

The following session details the members users within the privilege groups.

Domain Admins (2 Members)

Name	Last Logon Date	Password Never Expires	Account Enabled
Administrator	4/12/2024	**Yes	Yes
eddard.stark	4/12/2024	**Yes	Yes

Table 61 - Domain Admins - NORTH.SEVENKINGDOMS.LOCAL

Health Check:

Security Best Practice:

**Ensure there aren't any account with weak security posture.

Remote Desktop Users (9 Members)

Name	Last Logon Date	Password Never Expires	Account Enabled
arya.stark	--	**Yes	Yes
brandon.stark	--	**Yes	Yes
catelyn.stark	--	**Yes	Yes
eddard.stark	4/12/2024	**Yes	Yes
hodor	--	**Yes	Yes
jon.snow	--	**Yes	Yes
rickon.stark	--	**Yes	Yes
robb.stark	4/12/2024	**Yes	Yes
sansa.stark	--	**Yes	Yes

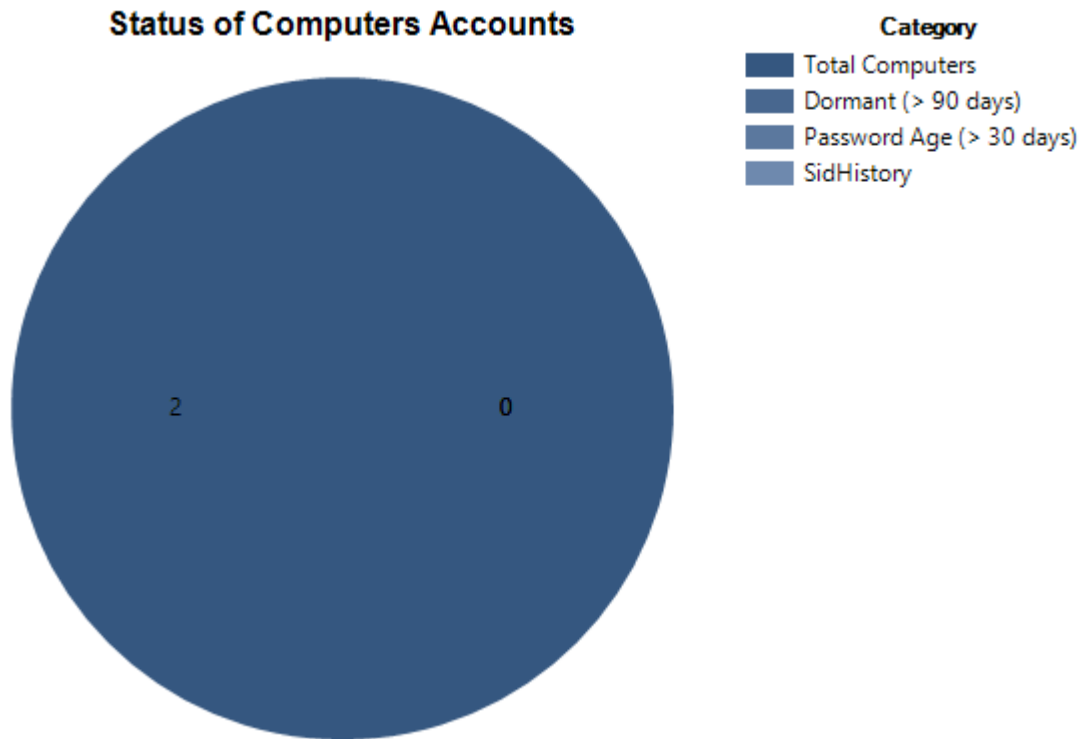
Table 62 - Remote Desktop Users - NORTH.SEVENKINGDOMS.LOCAL

Health Check:

Security Best Practice:

**Ensure there aren't any account with weak security posture.

2.2.6 Status of Computer Accounts



Category	Enabled	Enabled %	Disabled	Disabled %	Total	Total %
Total Computers	2	100	0	0	2	100
Dormant (> 90 days)	1	50	1	50	0	0
Password Age (> 30 days)	1	50	1	50	0	0
SidHistory	1	50	1	50	0	0

Table 63 - Status of Computer Accounts - NORTH.SEVENKINGDOMS.LOCAL

2.2.7 Operating Systems Count

Operating System	Count
Windows Server 2019 Datacenter Evaluation	2

Table 64 - Operating System Count - NORTH.SEVENKINGDOMS.LOCAL

2.2.8 Default Domain Password Policy

Password Must Meet Complexity Requirements	No
Path	north.sevenkingdoms.local/
Lockout Duration	05 minutes

Lockout Threshold	5
Lockout Observation Window	05 minutes
Max Password Age	37201 days
Min Password Age	01 days
Min Password Length	5
Enforce Password History	24
Store Password using Reversible Encryption	No

Table 65 - Default Domain Password Policy - NORTH.SEVENKINGDOMS.LOCAL

2.2.9 Foreign Security Principals

Name	Principal Name
NT AUTHORITY\INTERACTIVE	Users
NT AUTHORITY\Authenticated Users	Pre-Windows 2000 Compatible Access Users
NT AUTHORITY\IUSR	IIS_IUSRS
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Windows Authorization Access Group

Table 66 - Foreign Security Principals - NORTH.SEVENKINGDOMS.LOCAL

2.2.10 Health Checks

Sysvol Content Status

The following section details domain NORTH.SEVENKINGDOMS.LOCAL sysvol health status.

Extension	File Count	Size
.cmt	1	0.00 MB
.inf	2	0.00 MB
.INI	3	0.00 MB
.pol	3	0.00 MB
.ps1	2	0.00 MB

Table 67 - Sysvol Content Status - NORTH.SEVENKINGDOMS.LOCAL

Health Check:

Corrective Actions: Make sure Sysvol folder has no malicious extensions or unnecessary content.

Netlogon Content Status

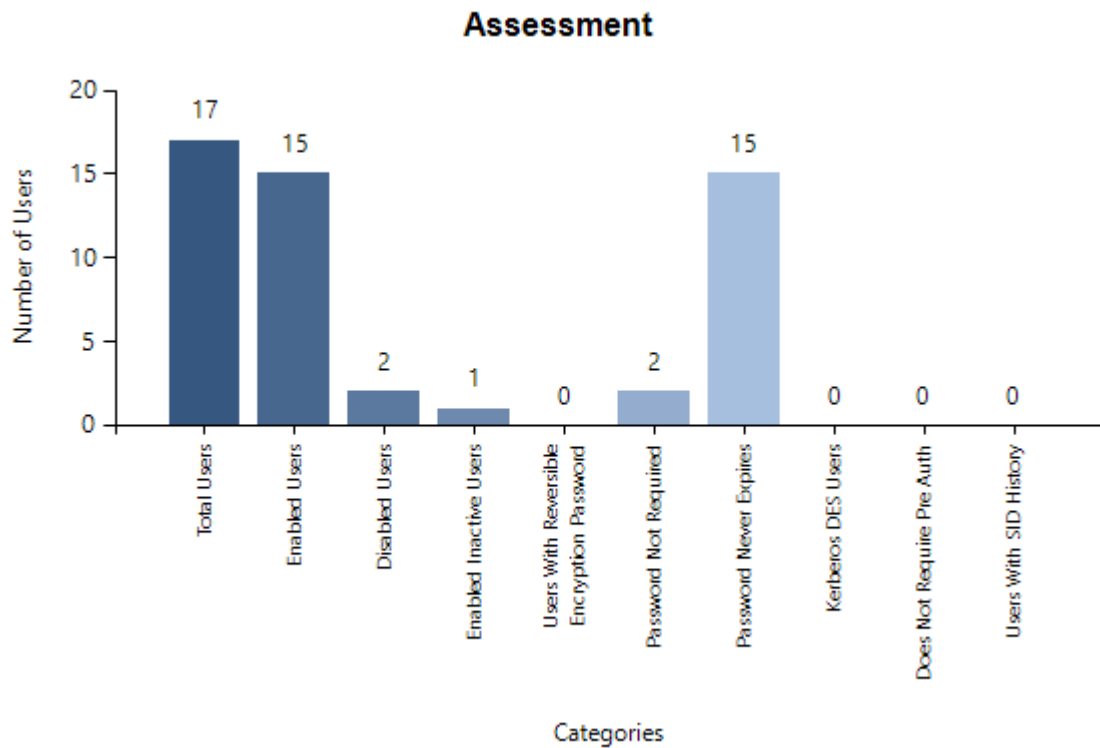
The following section details domain NORTH.SEVENKINGDOMS.LOCAL netlogon health status.

Extension	File Count	Size
.ps1	2	0.00 MB

Table 68 - Netlogon Content Status - NORTH.SEVENKINGDOMS.LOCAL

Account Security Assessment

The following section provide a summary of the Account Security Assessment on Domain NORTH.SEVENKINGDOMS.LOCAL.



Total Users	17
Enabled Users	15
Disabled Users	2
Enabled Inactive Users	1
Users With Reversible Encryption Password	0
Password Not Required	2
Password Never Expires	15
Kerberos DES Users	0
Does Not Require Pre Auth	0
Users With SID History	0

Table 69 - Account Security Assessment - NORTH.SEVENKINGDOMS.LOCAL

Health Check:

Corrective Actions: Ensure there aren't any account with weak security posture.

Privileged Users Assessment

The following section details probable AD Admin accounts (user accounts with AdminCount set to 1) on Domain NORTH.SEVENKINGDOMS.LOCAL

Username	Password Last Set	Last Logon Date	Email Enabled?	Trusted for Delegation
Administrator	4/12/2024	4/12/2024	No	** Yes
vagrant	5/12/2021	4/12/2024	No	** Yes
krbtgt	4/12/2024	--	No	** Yes
eddard.stark	4/12/2024	4/12/2024	No	** Yes
catelyn.stark	4/12/2024	--	No	** Yes
robb.stark	4/12/2024	4/12/2024	No	** Yes

Table 70 - Privileged User Assessment - NORTH.SEVENKINGDOMS.LOCAL

Health Check:

Security Best Practice:

** Privileged accounts such as those belonging to any of the administrator groups must not be trusted for delegation. Allowing privileged accounts to be trusted for delegation provides a means for privilege escalation from a compromised system. Delegation of privileged accounts must be prohibited. Reference: https://www.stigviewer.com/stig/active_directory_domain/2017-12-15/finding/V-36435

Service Accounts Assessment

The following section details probable AD Service Accounts (user accounts with SPNs) on Domain NORTH.SEVENKINGDOMS.LOCAL

Username	Enabled	Password Last Set	Last Logon Date	Service Principal Name
krbtgt	No	4/12/2024	--	kadmin/changepw
sansa.stark	Yes	4/12/2024	--	HTTP/eyrie.north.sevenkingdoms.local
jon.snow	Yes	4/12/2024	--	CIFS/thewall.north.sevenkingdoms.local HTTP/thewall.north.sevenkingdoms.local
sql_svc	Yes	4/12/2024	4/12/2024	MSSQLSvc/castelblack.north.sevenkingdoms.local MSSQLSvc/castelblack.north.sevenkingdoms.local:1433

Table 71 - Service Accounts Assessment - NORTH.SEVENKINGDOMS.LOCAL

Health Check:

KRBTGT Account Audit

The following section provide a summary of KRBTGT account on Domain NORTH.SEVENKINGDOMS.LOCAL.

Name	krbtgt
Created	04/12/2024 14:11:29
Password Last Set	04/12/2024 14:11:29
Distinguished Name	CN=krbtgt,CN=Users,DC=north,DC=sevenkingdoms,DC=local

Table 72 - KRBTGT Account Audit - NORTH.SEVENKINGDOMS.LOCAL

Health Check:

Best Practice: Microsoft advises changing the krbtgt account password at regular intervals to keep the environment more secure.

Administrator Account Audit

The following section provide a summary of Administrator account on Domain NORTH.SEVENKINGDOMS.LOCAL.

Name	Administrator
Created	04/12/2024 13:58:34
Password Last Set	04/12/2024 13:36:04
Last Logon Date	04/12/2024 14:18:50
Distinguished Name	CN=Administrator,CN=Users,DC=north,DC=sevenkingdoms,DC=local

Table 73 - Administrator Account Audit - NORTH.SEVENKINGDOMS.LOCAL

Health Check:

Best Practice: Microsoft advises changing the administrator account password at regular intervals to keep the environment more secure.

2.2.11 Domain Controllers

The following section provides detailed information about Active Directory domain controllers.

2.2.11.1 WINTERFELL

General Information

Microsoft Active Directory As Built Report - v1.0

DC Name	winterfell.north.sevenkingdoms.local
Domain Name	north.sevenkingdoms.local
Site	Default-First-Site-Name
Global Catalog	Yes
Read Only	No
Location	
Computer Object SID	S-1-5-21-3784733952-806722479-2510178485-1001
Operating System	Windows Server 2019 Datacenter Evaluation
Description	

Table 74 - General Information - WINTERFELL

Partitions

Default Partition	DC=north,DC=sevenkingdoms,DC=local
Partitions	DC=DomainDnsZones,DC=north,DC=sevenkingdoms,DC=local DC=north,DC=sevenkingdoms,DC=local DC=ForestDnsZones,DC=sevenkingdoms,DC=local CN=Schema,CN=Configuration,DC=sevenkingdoms,DC=local CN=Configuration,DC=sevenkingdoms,DC=local DC=sevenkingdoms,DC=local

Table 75 - Partitions - WINTERFELL

Networking Settings

IPv4 Addresses	--
IPv6 Addresses	--
LDAP Port	389
SSL Port	636

Table 76 - Networking Settings - WINTERFELL

Hardware Inventory

Name	WINTERFELL
Windows Product Name	Windows Server 2019 Datacenter Evaluation
Windows Build Number	10.0.17763
AD Domain	north.sevenkingdoms.local
Windows Installation Date	04/12/2024 10:56:07
Time Zone	(UTC-04:00) Georgetown, La Paz, Manaus, San Juan
License Type	Retail:TB:Eval
Partial Product Key	H6F8M
Manufacturer	VMware, Inc.

Model	VMware Virtual Platform
Processor Model	Intel(R) Core(TM) i7-6700 CPU @ 3.40GHz
Number of Processors	4
Number of CPU Cores	1
Number of Logical Cores	1
Physical Memory	5.86 GB

Table 77 - Hardware Inventory - WINTERFELL

Health Check:

Best Practice: Microsoft recommend putting enough RAM 8GB+ to load the entire DIT into memory, plus accommodate the operating system and other installed applications, such as anti-virus, backup software, monitoring, and so on.

2.2.11.2 DNS IP Configuration

DC Name	Interface	Preferred DNS	Alternate DNS	DNS 3	DNS 4
WINTERFELL	Ethernet0	127.0.0.1	192.168.5.1	8.8.8.8	--
WINTERFELL	Ethernet1	127.0.0.1	192.168.56.10	--	--

Table 78 - DNS IP Configuration - NORTH.SEVENKINGDOMS.LOCAL

Health Check:

Best Practices: DNS configuration on network adapter should include the loopback address, but not as the first entry.

Corrective Actions: Network interfaces must be configured with DNS servers that can resolve names in the forest root domain. The following DNS server did not respond to the query for the forest root domain NORTH.SEVENKINGDOMS.LOCAL: 8.8.8.8

2.2.11.3 NTDS Information

DC Name	Database File	Database Size	Log Path	SysVol Path
WINTERFELL	C:\Windows\NTDS\ntds.dit	22.00 MB	C:\Windows\Logs	C:\Windows\SYSTEM32\sysvol

Table 79 - NTDS Database File Usage - NORTH.SEVENKINGDOMS.LOCAL

2.2.11.4 Time Source Information

Name	Time Server	Type
WINTERFELL	Domain Hierarchy	DOMHIER

Table 80 - Time Source Configuration - NORTH.SEVENKINGDOMS.LOCAL

2.2.11.5 SRV Records Status

Name	A Record	KDC SRV	PDC SRV	GC SRV	DC SRV
WINTERFELL	OK	OK	OK	OK	OK

Table 81 - SRV Records Status - NORTH.SEVENKINGDOMS.LOCAL

2.2.11.6 Roles

The following section provides a summary of installed role & features on north.sevenkingdoms.local DCs.

WINTERFELL

Name	Parent	Description
Active Directory Domain Services	Role	Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.
DNS Server	Role	Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.
File and Storage Services	Role	File and Storage Services includes services that are always installed, as well as functionality that you can install to help manage file servers and storage.

Table 82 - Roles - WINTERFELL

2.2.11.7 DC Diagnostic

The following section provides a summary of the Active Directory DC Diagnostic.

WINTERFELL

Test Name	Result	Impact	Description
Replications	Passed	High	Makes a deep validation to check the main replication for all naming contexts in this Domain Controller.
RidManager	Passed	High	Validates this Domain Controller can locate and contact the RID Master FSMO role holder. This test is skipped in RODCs.
ObjectsReplicated	Passed	High	Checks the replication health of core objects and attributes.

Microsoft Active Directory As Built Report - v1.0

Test Name	Result	Impact	Description
NCSecDesc	Passed	Medium	Validates if permissions are correctly set in this Domain Controller for all naming contexts. Those permissions directly affect replications health.
NetLogons	Passed	High	Validates if core security groups (including administrators and Authenticated Users) can connect and read NETLOGON and SYSVOL folders. It also validates access to IPC\$. which can lead to failures in organizations that disable IPC\$.
Services	Passed	High	Validates if the core Active Directory services are running in this Domain Controller. The services verified are: RPCSS, EVENTSYSTEM, DNSCACHE, ISMSERV, KDC, SAMSS, WORKSTATION, W32TIME, NETLOGON, NTDS (in case Windows Server 2008 or newer) and DFSR (if SYSVOL is using DFSR).
VerifyReplicas	Passed	High	Checks that all application directory partitions are fully instantiated on all replica servers.
DNS	Passed	Medium	DNS Includes six optional DNS-related tests, as well as the Connectivity test, which runs by default.
VerifyReferences	Passed	High	Validates that several attributes are present for the domain in the container and subcontainers in the DC objects. This test will fail if any attribute is missing.
SystemLog	Failed	Low	Checks if there is any errors in the Event Viewer > System event log in the past 60 minutes. Since the System event log records data from many places, errors reported here may lead to false positive and must be investigated further. The impact of this validation is marked as Low.
Topology	Passed	Medium	Topology Checks that the KCC has generated a fully connected topology for all domain controllers.
CutoffServers	Passed	Medium	Checks for any server that is not receiving replications because its partners are not running
FrsEvent	Passed	Medium	Checks if theres any errors in the event logs regarding FRS replication. If running Windows Server 2008 R2 or newer on all Domain Controllers is possible SYSVOL were already migrated to DFSR, in this case errors found here can be ignored.
CheckSecurityError	Passed	Medium	Reports on the overall health of replication with respect to Active Directory security in domain controllers running Windows Server 2003 SP1.
Connectivity	Passed	Medium	Initial connection validation, checks if the DC can be located in the DNS, validates the ICMP ping (1 hop), checks LDAP binding and also the RPC connection. This initial test requires ICMP, LDAP, DNS and RPC connectivity to work properly.
Advertising	Passed	High	Validates this Domain Controller can be correctly located through the KDC service. It does not validate the

Microsoft Active Directory As Built Report - v1.0

Test Name	Result	Impact	Description
			Kerberos tickets answer or the communication through the TCP and UDP port 88.
DFSREvent	Failed	Medium	Checks if theres any errors in the event logs regarding DFSR replication. If running Windows Server 2008 or older on all Domain Controllers is possible SYSVOL is still using FRS, and in this case errors found here can be ignored. Obs. is highly recommended to migrate SYSVOL to DFSR.
KnowsOfRoleHolders	Passed	High	Checks if this Domain Controller is aware of which DC (or DCs) hold the FSMOs.
MachineAccount	Passed	High	Checks if this computer account exist in Active Directory and the main attributes are set. If this validation reports error. the following parameters of DCDIAG might help: /RecreateMachineAccount and /FixMachineAccount.
KccEvent	Passed	High	Validates through KCC there were no errors in the Event Viewer > Applications and Services Logs > Directory Services event log in the past 15 minutes (default time).
SysVolCheck	Passed	High	Validates if the registry key HKEY_Local_Machine\System\CurrentControlSet\Services\Netlogon\Parameters\SysvolReady=1 exist. This registry has to exist with value 1 for the DCs SYSVOL to be advertised.
FrsSysVol	Passed	Medium	Checks that the file replication system (FRS) system volume (SYSVOL) is ready

Table 83 - DCDiag Test Status - WINTERFELL

2.2.11.8 Infrastructure Services

The following section provides a summary of the Domain Controller Infrastructure services status.

WINTERFELL

Display Name	Short Name	Status
Active Directory Domain Services	NTDS	Running
Active Directory Web Services	ADWS	Running
COM+ Event System	EVENTSYSTEM	Running
DFS Replication	DFSR	Running
DNS Client	DNSCACHE	Running
DNS Server	DNS	Running
Intersite Messaging	IsmServ	Running
Kerberos Key Distribution Center	Kdc	Running
NetLogon	Netlogon	Running
Print Spooler	Spooler	Running

Display Name	Short Name	Status
Remote Procedure Call (RPC)	RPCSS	Running
Security Accounts Manager	SAMSS	Running
Windows Time	W32Time	Running
WORKSTATION	LanmanWorkstation	Running

Table 84 - Infrastructure Services Status - WINTERFELL

Health Check:

Corrective Actions: Disable Print Spooler service on DCs and all servers that do not perform Print services.

2.2.12 Replication Connection

The following section provides detailed information about Replication Connection.

Site: Default-First-Site-Name: From: KINGSLANDING To: WINTERFELL

Name	<automatically generated>
From Site	Default-First-Site-Name
GUID	aaf9f7e0-1185-49ba-ada3-0005443d0564
Description	--
From Server	KINGSLANDING
To Server	WINTERFELL
Replicated Naming Contexts	DC=DomainDnsZones,DC=north,DC=sevenkingdoms,DC=local DC=north,DC=sevenkingdoms,DC=local DC=ForestDnsZones,DC=sevenkingdoms,DC=local CN=Schema,CN=Configuration,DC=sevenkingdoms,DC=local CN=Configuration,DC=sevenkingdoms,DC=local
Transport Protocol	
Auto Generated	Yes
Enabled	Yes
Created	Fri, 12 Apr 2024 18:12:39 GMT

Table 85 - Replication Connection - WINTERFELL

2.2.13 Replication Status

From Server	To Server	From Site	Last Success Time	Last Failure Status	Last Failure Time	Failures
KINGSLANDI NG	WINTERFELL	Default-First- Site-Name	2024-04-13 01:17:31	0	0	0

Microsoft Active Directory As Built Report - v1.0

From Server	To Server	From Site	Last Success Time	Last Failure Status	Last Failure Time	Failures
KINGSLANDI-NG	WINTERFELL	Default-First-Site-Name	2024-04-13 01:17:31	0	0	0
KINGSLANDI-NG	WINTERFELL	Default-First-Site-Name	2024-04-13 01:17:31	0	0	0
KINGSLANDI-NG	WINTERFELL	Default-First-Site-Name	2024-04-13 01:17:31	0	0	0

Table 86 - Replication Status - NORTH.SEVENKINGDOMS.LOCAL

2.2.14 Group Policy Objects

The following section provides a summary of the Group Policy Objects for domain NORTH.SEVENKINGDOMS.LOCAL.

Default Domain Policy

GPO Status	All Settings Enabled
GUID	31b2f340-016d-11d2-945f-00c04fb984f9
Created	04/12/2024
Modified	04/12/2024
Owner	NORTH\Domain Admins
Computer Version	4 (AD), 4 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	north.sevenkingdoms.local
Description	--

Table 87 - GPO - Default Domain Policy

StarkWallpaper

GPO Status	All Settings Enabled
GUID	52693def-fe84-47db-862e-67cc1b473a20
Created	04/12/2024
Modified	04/12/2024
Owner	NORTH\vagrant
Computer Version	1 (AD), 1 (SYSVOL)
User Version	2 (AD), 2 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	north.sevenkingdoms.local

Description	Change Wallpaper
-------------	------------------

Table 88 - GPO - StarkWallpaper

Default Domain Controllers Policy

GPO Status	All Settings Enabled
GUID	6ac1786c-016f-11d2-945f-00c04fb984f9
Created	04/12/2024
Modified	04/12/2024
Owner	NORTH\Domain Admins
Computer Version	1 (AD), 1 (SYSVOL)
User Version	0 (AD), 0 (SYSVOL)
WMI Filter	--
Security Filtering	Authenticated Users
Linked Target	north.sevenkingdoms.local/Domain Controllers
Description	--

Table 89 - GPO - Default Domain Controllers Policy

2.2.14.1 Central Store Repository

Domain	Configured	Central Store Path
NORTH.SEVENKINGDOMS.LOCAL	No	\\north.sevenkingdoms.local\SYSVOL\north.sevenkingdoms.local\Policies\PolicyDefinitions

Table 90 - GPO Central Store - NORTH.SEVENKINGDOMS.LOCAL

Health Check:

Best Practices: The group policy central store is a central location to store all the group policy template files. This eliminates the need for admins to load and open group policy template files on systems used to manage group policy. Ensure Central Store is deployed to centralized GPO repository.

2.2.15 Organizational Units

The following section provides a summary of Active Directory Organizational Unit information.

Name	Linked GPO	Protected
Domain Controllers	Default Domain Controllers Policy	No

Table 91 - Organizational Unit - NORTH.SEVENKINGDOMS.LOCAL

Health Check:

Best Practice: If the Organizational Units in your Active Directory are not protected from accidental deletion, your environment can experience disruptions that might be caused by accidental bulk deletion of objects. All OUs in this domain should be protected from accidental deletion

3 DNS Configuration

The following section provides a summary of the Active Directory DNS Infrastructure Information.

3.1 SEVENKINGDOMS.LOCAL

The following section provides a configuration summary of the DNS service.

3.1.1 Infrastructure Summary

The following section provides a summary of the DNS Infrastructure configuration.

DC Name	Build Number	IPv6	DnsSec	ReadOnly DC	Listening IP
KINGSLANDING	17763	Yes	Yes	No	192.168.56.10

Table 92 - Infrastructure Summary - SEVENKINGDOMS.LOCAL

3.1.1.1 Application Directory Partition

The following section provides Directory Partition information.

KINGSLANDING

Name	State	Flags	Zone Count
DomainDnsZones.north.sevenkingdoms.local	--	Not-Enlisted	0
DomainDnsZones.sevenkingdoms.local	DNS_DP_OKAY	Enlisted Auto Domain	2
ForestDnsZones.sevenkingdoms.local	DNS_DP_OKAY	Enlisted Auto Forest	2

Table 93 - Directory Partitions - KINGSLANDING

3.1.1.2 Response Rate Limiting (RRL)

DC Name	Status	Responses Per Sec	Errors Per Sec	Window In Sec	Leak Rate	Truncate Rate
KINGSLANDING	Disable	5	5	5	3	2

Table 94 - Response Rate Limiting - SEVENKINGDOMS.LOCAL

3.1.1.3 Scavenging Options

DC Name	NoRefresh Interval	Refresh Interval	Scavenging Interval	Last Scavenge Time	Scavenging State
KINGSLANDING	7.00:00:00	7.00:00:00	00:00:00	--	Disabled

Table 95 - Scavenging - SEVENKINGDOMS.LOCAL

Health Check:

Best Practices: Microsoft recommends to enable aging/scavenging on all DNS servers. However, with AD-integrated zones ensure to enable DNS scavenging on one DC at main site. The results will be replicated to other DCs.

3.1.1.4 Forwarder Options

DC Name	IP Address	Timeout	Use Root Hint	Use Recursion
KINGSLANDING	1.1.1.1 9.9.9.9	3/s	No	Yes

Table 96 - Forwarders - SEVENKINGDOMS.LOCAL

Health Check:

Best Practices: Configure the servers to use no more than two external DNS servers as Forwarders.

Reference: <https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/forwarders-resolution-timeouts>

3.1.1.5 Root Hints

The following section provides Root Hints information from domain sevenkingdoms.local.

KINGSLANDING

Name	IPv4 Address	IPv6 Address
a.root-servers.net.	198.41.0.4	2001:503:ba3e::2:30
b.root-servers.net.	--	2801:1b8:10::b
c.root-servers.net.	--	2001:500:2::c
d.root-servers.net.	--	2001:500:2d::d
e.root-servers.net.	--	2001:500:a8::e
f.root-servers.net.	--	2001:500:2f::f
g.root-servers.net.	--	2001:500:12::d0d
h.root-servers.net.	--	2001:500:1::53
i.root-servers.net.	--	2001:7fe::53
j.root-servers.net.	--	2001:503:c27::2:30

Name	IPv4 Address	IPv6 Address
k.root-servers.net.	--	2001:7fd::1
l.root-servers.net.	--	2001:500:9f::42
m.root-servers.net.	--	2001:dc3::35

Table 97 - Root Hints - KINGSLANDING

3.1.1.6 Zone Scope Recursion

DC Name	Zone Name	Forwarder	Use Recursion
KINGSLANDING	Root	1.1.1.1 9.9.9.9	Yes

Table 98 - Zone Scope Recursion - SEVENKINGDOMS.LOCAL

3.1.2 KINGSLANDING DNS Zones

Zone Name	Zone Type	Replication Scope	Dynamic Update	DS Integrated	Read Only	Signed
_msdcs.sevenkingdoms.local	Primary	Forest	Secure	Yes	No	No
sevenkingdoms.local	Primary	Domain	Secure	Yes	No	No

Table 99 - Zones - SEVENKINGDOMS.LOCAL

3.1.2.1 Zone Delegation

Zone Name	Child Zone	Name Server	IP Address
sevenkingdoms.local	_msdcs.sevenkingdoms.local.	kingslanding.sevenkingdoms.local.	192.168.56.10

Table 100 - Zone Delegations - SEVENKINGDOMS.LOCAL

3.1.2.2 Reverse Lookup Zone

Zone Name	Zone Type	Replication Scope	Dynamic Update	DS Integrated	Read Only	Signed
0.in-addr.arpa	Primary	None	None	No	No	No
127.in-addr.arpa	Primary	None	None	No	No	No
255.in-addr.arpa	Primary	None	None	No	No	No

Table 101 - Zones - SEVENKINGDOMS.LOCAL

3.1.2.3 Conditional Forwarder

Zone Name	Zone Type	Replication Scope	Master Servers	DS Integrated
essos.local	Forwarder	Forest	192.168.56.12	Yes

Table 102 - Conditional Forwarders - SEVENKINGDOMS.LOCAL

3.1.2.4 Zone Scope Aging

Zone Name	Aging Enabled	Refresh Interval	NoRefresh Interval	Available For Scavenge
_msdcs.sevenkingdoms.local	No	7.00:00:00	7.00:00:00	--
sevenkingdoms.local	No	7.00:00:00	7.00:00:00	--

Table 103 - Zone Aging Properties - SEVENKINGDOMS.LOCAL

Health Check:

Best Practices: Microsoft recommends to enable aging/scavenging on all DNS servers. However, with AD-integrated zones ensure to enable DNS scavenging on one DC at main site. The results will be replicated to other DCs.

3.2 NORTH.SEVENKINGDOMS.LOCAL

The following section provides a configuration summary of the DNS service.

3.2.1 Infrastructure Summary

The following section provides a summary of the DNS Infrastructure configuration.

DC Name	Build Number	IPv6	DnsSec	ReadOnly DC	Listening IP
WINTERFELL	17763	Yes	Yes	No	192.168.56.11

Table 104 - Infrastructure Summary - NORTH.SEVENKINGDOMS.LOCAL

3.2.1.1 Application Directory Partition

The following section provides Directory Partition information.

WINTERFELL

Name	State	Flags	Zone Count
DomainDnsZones.north.sevenkingdoms.local	DNS_DP_OKAY	Enlisted Auto Domain	2
DomainDnsZones.sevenkingdoms.local	--	Not-Enlisted	0
ForestDnsZones.sevenkingdoms.local	DNS_DP_OKAY	Enlisted Auto Forest	2

Table 105 - Directory Partitions - WINTERFELL

3.2.1.2 Response Rate Limiting (RRL)

DC Name	Status	Responses Per Sec	Errors Per Sec	Window In Sec	Leak Rate	Truncate Rate
WINTERFELL	Disable	5	5	5	3	2

Table 106 - Response Rate Limiting - NORTH.SEVENKINGDOMS.LOCAL

3.2.1.3 Scavenging Options

DC Name	NoRefresh Interval	Refresh Interval	Scavenging Interval	Last Scavenge Time	Scavenging State
WINTERFELL	7.00:00:00	7.00:00:00	00:00:00	--	Disabled

Table 107 - Scavenging - NORTH.SEVENKINGDOMS.LOCAL

Health Check:

Best Practices: Microsoft recommends to enable aging/scavenging on all DNS servers. However, with AD-integrated zones ensure to enable DNS scavenging on one DC at main site. The results will be replicated to other DCs.

3.2.1.4 Forwarder Options

DC Name	IP Address	Timeout	Use Root Hint	Use Recursion
WINTERFELL	192.168.5.1 8.8.8.8 192.168.56.10	3/s	Yes	Yes

Table 108 - Forwarders - NORTH.SEVENKINGDOMS.LOCAL

Health Check:

Best Practices: Configure the servers to use no more than two external DNS servers as Forwarders.

Reference: <https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/forwarders-resolution-timeouts>

3.2.1.5 Root Hints

The following section provides Root Hints information from domain north.sevenkingdoms.local.

WINTERFELL

Name	IPv4 Address	IPv6 Address
a.root-servers.net.	198.41.0.4	2001:503:ba3e::2:30
b.root-servers.net.	--	2801:1b8:10::b
c.root-servers.net.	--	2001:500:2::c
d.root-servers.net.	--	2001:500:2d::d
e.root-servers.net.	--	2001:500:a8::e
f.root-servers.net.	--	2001:500:2f::f
g.root-servers.net.	--	2001:500:12::d0d
h.root-servers.net.	--	2001:500:1::53
i.root-servers.net.	--	2001:7fe::53
j.root-servers.net.	--	2001:503:c27::2:30
k.root-servers.net.	--	2001:7fd::1
l.root-servers.net.	--	2001:500:9f::42
m.root-servers.net.	--	2001:dc3::35

Table 109 - Root Hints - WINTERFELL

3.2.1.6 Zone Scope Recursion

DC Name	Zone Name	Forwarder	Use Recursion
WINTERFELL	Root	192.168.5.1 8.8.8.8 192.168.56.10	Yes

Table 110 - Zone Scope Recursion - NORTH.SEVENKINGDOMS.LOCAL

3.2.2 WINTERFELL DNS Zones

Zone Name	Zone Type	Replication Scope	Dynamic Update	DS Integrated	Read Only	Signed
_msdcs.sevenkingdoms.local	Primary	Forest	Secure	Yes	No	No
north.sevenkingdoms.local	Primary	Domain	Secure	Yes	No	No

Table 111 - Zones - NORTH.SEVENKINGDOMS.LOCAL

3.2.2.1 Reverse Lookup Zone

Zone Name	Zone Type	Replication Scope	Dynamic Update	DS Integrated	Read Only	Signed
0.in-addr.arpa	Primary	None	None	No	No	No
127.in-addr.arpa	Primary	None	None	No	No	No
255.in-addr.arpa	Primary	None	None	No	No	No

Table 112 - Zones - NORTH.SEVENKINGDOMS.LOCAL

3.2.2.2 Conditional Forwarder

Zone Name	Zone Type	Replication Scope	Master Servers	DS Integrated
essos.local	Forwarder	Forest	192.168.56.12	Yes
sevenkingdoms.local	Forwarder	None	192.168.56.10	No

Table 113 - Conditional Forwarders - NORTH.SEVENKINGDOMS.LOCAL

3.2.2.3 Zone Scope Aging

Zone Name	Aging Enabled	Refresh Interval	NoRefresh Interval	Available For Scavenge
_msdcs.sevenkingdoms.local	No	7.00:00:00	7.00:00:00	--
north.sevenkingdoms.local	No	7.00:00:00	7.00:00:00	--

Table 114 - Zone Aging Properties - NORTH.SEVENKINGDOMS.LOCAL

Health Check:

Best Practices: Microsoft recommends to enable aging/scavenging on all DNS servers. However, with AD-integrated zones ensure to enable DNS scavenging on one DC at main site. The results will be replicated to other DCs.