novaCapta

Whitepaper

Health Check Ihres Active Directory

Einblick in Teile unserer Ergebnisdokumentation

DE

novaCapta GmbH
Im Mediapark 5c
50670 Köln

T +49 (0)221 58919 343
M info@novacapta.com
W www.novacapta.com

CH

novaCapta Schweiz AG
Industriestrasse 5a
6210 Sursee

T +41 (0)41 392 20 00
M info.schweiz@novacapta.com
W www.novacapta.ch

Fehlerfreie Services und Prozesse

Die Active Directory ist das Herz Ihrer Microsoft Windows-basierten IT-Infrastruktur. Damit es fehlerfrei schlägt, führen wir für Sie einen umfangreichen Health Check durch. Er umfasst alle Bereiche, die für die Leistung, Stabilität und Sicherheit aller damit verbundenen Anwendungen, Services und Prozesse wichtig sind.

Das dokumentierte Ergebnis Ihres Active Directory Domain Services Health Checks erhalten Sie in Form eines Ergebnispapiers. Und damit Sie sich besser vorstellen können, was unser Service alles beinhaltet, bietet Ihnen diese kostenlose Demo einen detaillierten Einblick in die Analyseobjekte, den Aufbau und empfohlene Maßnahmen unseres Health Checks.

So wissen Sie als Kunde gleich, wie es um die Gesundheit Ihrer Active Directory steht und was Sie aktiv tun können, um den Zustand zu halten oder zu verbessern.

Zusammenfassung der Health Check Ergebnisse

Die Zusammenfassung der Health Check Ergebnisse gibt vor, inwiefern ein Handlungsbedarf in Bezug auf die Konfigurationder Active Directory Gesamtstruktur besteht und unterstützt mitkonkreten Handlungsempfehlungen.

Thema	Kurzbeschreibung	Empfehlung	Handlungsbedarf
Active Directory	Aktivierung des Active Directory-Papierkorbs	Aktivieren der Funktionalität des Active Directory-Papierkorbs für die Gesamtstruktur	Niedrig
Active Directory	Erstellung eines Key Distribution Service-Stammschlüssels	Erstellen eines Key Distribution Service-Stammschlüssels zur Verwendung weiterer Funktionalitäten	Optional
Active Directory	Überprüfung der Tombstome Lifetime	Anheben des Wertes für die Tombstome Lifetime auf den Stanardwert von 180 Tagen	Optional
Active Directory	Quota für das Hinzufügen von Computerkonten	Herabsetzen des Wertes auf 0	Mittel
...	...	...	...
Active Directory	Überprüfung von Gruppenrichtlinienanteilen	Deaktvieren von nicht genutzten Richtlinienanteilen	Niedrig
Active Directory	Überprüfung von deaktivierten Gruppenrichtlinien	Überprüfen von deaktivierten Richtlinien, ob deren Verknüpfung weiterhin benötigt wird	Niedrig
...	...	...	...
Active Directory	Überprüfung von Computerkonten	Überprüfen von Computerkonten, die seit 90 Tagen keine Anmeldung mehr protokolliert haben, keinen Anmeldezeitstempel besitzen oder einen unerwarteten Betriebssystemwert haben	Niedrig
Active Directory	Überprüfung von Computerkonten	Überprüfen der Computerkonten mit nicht mehr unterstütztem Windows Server Betriebssystem	Niedrig
Active Directory	Überprüfung von Computerkonten	Überprüfen der Computerkonten mit nicht mehr unterstütztem Windows Desktop Betriebssystem	Niedrig
...	...	...	...
Betriebssystem	Aktualisierung des .NET Frameworks	Aktualisierung der .NET Framework Installationsversion über alle Windows Server 2016-basierenden Domänencontroller	Niedrig
Betriebssystem	SMBv1 Konfiguration	Deaktivieren des SMBv1 Protokolls für den SMB-Client und -Server	Mittel
Betriebssystem	Verwendung der Server Core Installationsvariante	Einsetzen der Server Core Installationsvariante für einen geringeren Ressourcenverbrauch und Angriffsfläche	Optional
...	...	...	...
DNS	Verschiebung der DNS-Zonen aus der Domänenpartition	Verschiebden von DNS-Zonen, die in der Domänenpartition gespeichert sind, in eine Anwendungspartition	Optional

Active Directory Gesamtstruktur

Die Active Directory-Domänendienste bieten unter Windows Server die Möglichkeit, eine AD-Gesamtstruktur aufzubauen. Diese ermöglicht die Verwaltung und Speicherung von Informationen über Ressourcen von einem Netzwerk und von Anwendungsdaten in einer verteilten Datenbank. Zudem müssen sämtliche Gruppenrichtlinien korrekt über alle Domänencontroller hinweg synchronisiert werden.

Allgemeine Information	
Stammdomäne	DC=contoso,DC=com
Erstinstallation	25.02.2003
Gesamtstrukturfunktionsebene	Windows Server 2008 R2
Domänen in Gesamtstruktur	1
Verzeichnispartitionen	5
Standorte	3
Domänencontroller und RODC	9
Schreibgeschützte Domänencontroller (RODC)	
Globale Katalogserver	9
Tombstone Lifetime	60 Tage
Active Directory Papierkorb	✗
Aufbewahrungszeit für gelöschte Objekte	
Privileged Access Management	
Key Distribution Service-Stammschlüssel	Nicht Verfügbar
Maximale Seitengröße für LDAP-Suchanfragen	1.000
Verzeichnisdienst Heuristiken	Standard
Alternative Benutzerprinzipalnamen-Suffixe	Keine
Alternative Dienstprinzipalnamen-Suffixe	Keine

Informationen zu Microsoft Exchange	
Name der Organisation	CONTOSO
Betriebsmodus	Einheitlicher Modus

Empfohlene Maßnahmen

1. Der Active Directory-Papierkorb ist in der Gesamtstruktur nicht aktiviert. Mit der Funktionalität des Active Directory-Papierkorbs können einzelne gelöschte Objekte in einem definierten Zeitraum vollständig wiederhergestellt werden, ohne das eine zusätzliche Sicherungssoftware zum Einsatz kommt. Der Aktivierungvorgang für den Active Directory-Papierkorbs kann nicht rückgängig gemacht werden. Trotzdem sollte diese Funktionalität aktiviert werden, um die Vorteile für einen ungewollten Löschvorgang nutzen zu können.

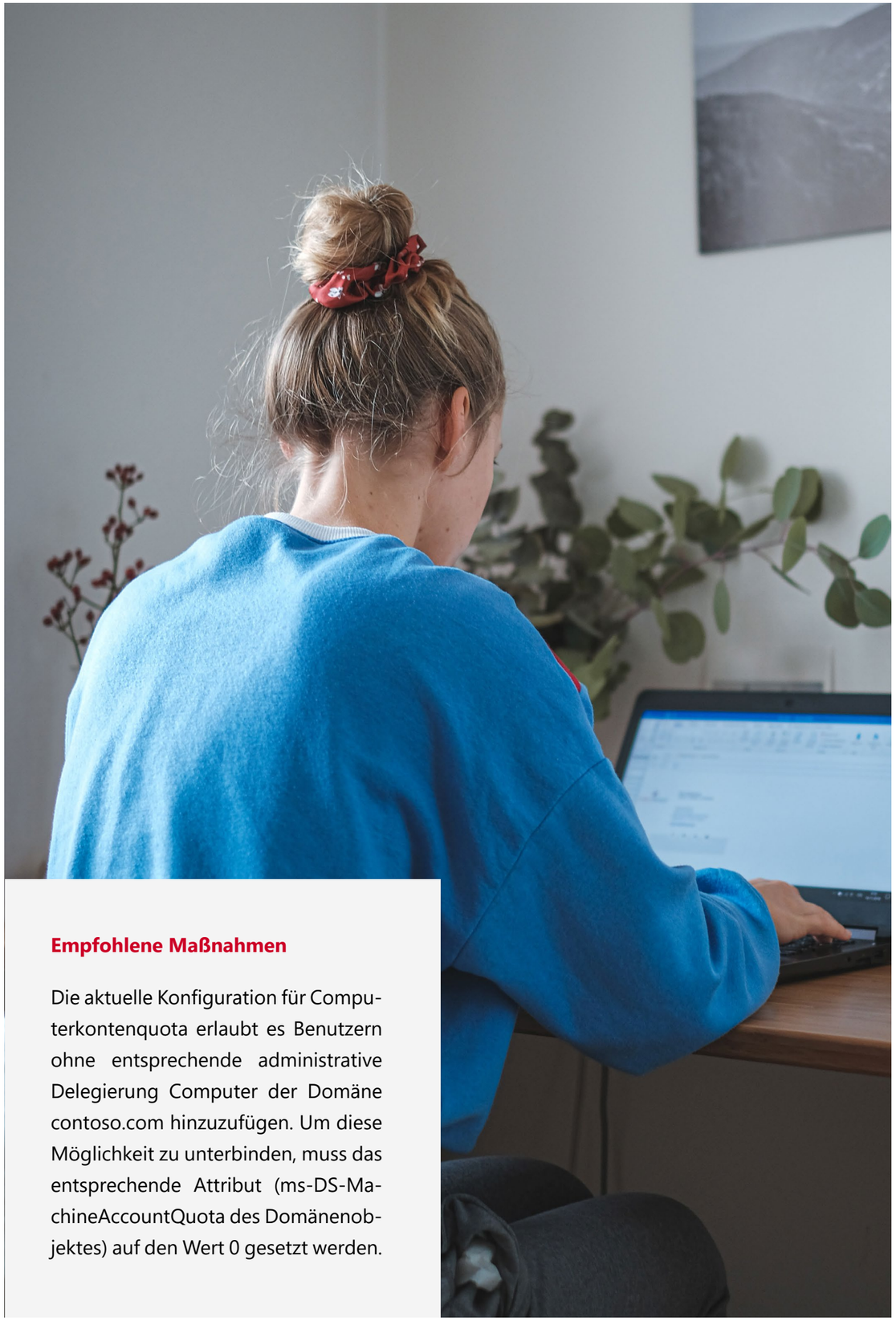
2. (Optional) Ein Key Distribution Service-Stammschlüssel wird zur Erstellung von „Managed Service Accounts" bzw. „Group Managed Service Accounts" benötigt, damit ein entsprechend sicheres Kennwort erstellt und in regelmäßigen Abständen geändert werden kann. Wenn der Einsatz dieser Funktionaliät geplant ist, dann sollte der Stammschlüssel im Vorfeld generiert werden, da dieser nicht sofort aktiv ist.

3. (Optional) Die Tombstone Life beschreibt den Zeitraum in dem ein Objekt nach seiner Löschung noch in der Active Directory Datenbank verbleibt bevor es endgültig entfernt wird. Bei einem aktiviertem Active Directory Papierkorb bestimmt der genannte Wert auch standardmäßig die Aufbewahrungszeit für Objekte im Papierkorb. Mit Windows 2000 Server wurde ein Standardwert von 60 Tagen eingeführt, der in späteren Versionen bei Neuinstallationen auf 180 Tage angehoben wurde. Sofern ein längeres Intervall gewünscht ist, sollte der neue Standardwert verwendet werden.

Domäne

Das Active Directory umfasst mindestens eine Domäne. Jede Domäne verfügt über ihren eigenen Sicherheitsbereich mit Richtlinien und Beziehungen, die festlegen, welche*r Mitarbeitende sich mit welchem Passwort anmelden und auf welche Objekte diese*r Zugriff haben darf. Inwiefern die Sicherheitsrichtlinien aktuell sind und welche Möglichkeiten besteht, zeigt dieses Kapitel.

Allgemeine Information	
Domänenname	DC=contoso,DC=com
DNS-Domänenname	contoso.com
NetBIOS-Domänenname	CONTOSO
Domänen-SID	S-1-5-21-1562428253-2244823749-249562893
Erstinstallation	25.02.2003
Domänenfunktionsebene	Windows Server 2008 R2
Domänencontroller und RODC	9
Schreibgeschützte Domänencontroller (RODC)	
Domänencontroller Betriebssysteme	Windows Server 2008 R2 Enterprise Windows Server 2008 R2 Standard Windows Server 2012 R2 Standard Windows Server 2016 Standard
Standard Container für Computerkonten	CN=Computers,DC=contoso,DC=com
Standard Container für Benutzerkonten	CN=Users,DC=contoso,DC=com
Quota für Computerkonten	10 (Standardwert)
LAN Manager User Account System (UAS) Kompatibilität	Aktiviert (Standardwert)
Alternative DNS-Suffixe	Keine



Empfohlene Maßnahmen

Die aktuelle Konfiguration für Computerkontenquota erlaubt es Benutzern ohne entsprechende administrative Delegierung Computer der Domäne contoso.com hinzuzufügen. Um diese Möglichkeit zu unterbinden, muss das entsprechende Attribut (ms-DS-MachineAccountQuota des Domänenobjektes) auf den Wert 0 gesetzt werden.

Gruppenrichtlinien

Eine Analyse der Gruppenrichtlinien empfehlen wir vor allem für in die Domäne eingebundene Client-Geräte, da sie eine detailliertere Kontrolle ermöglichen als andere Lösungen, wie z. B. PowerShell.

Information zu Gruppenrichtlinien	
Zentrale Ablage für Richtliniendefinitionen	✓
Anzahl an Gruppenrichtlinien in der Domäne	214
Anzahl an WMI-Filterdefinitionen	12
Gruppenrichtlinien Ersteller	NT AUTHORITY\SYSTEM CONTOSO\Domänen-Admins CONTOSO \Richtlinien-Ersteller-Besitzer CONTOSO \Exchange Servers (Vererbt) CONTOSO \Exchange Windows Permissions (Vererbt) CONTOSO \Exchange Trusted Subsystem (Vererbt) CONTOSO \Organization Management (Vererbt) CONTOSO \Organisations-Admins (Vererbt) S-1-5-21-1292428093-1844823847-839522115-527 (Vererbt) BUILTIN\Administratoren (Vererbt)

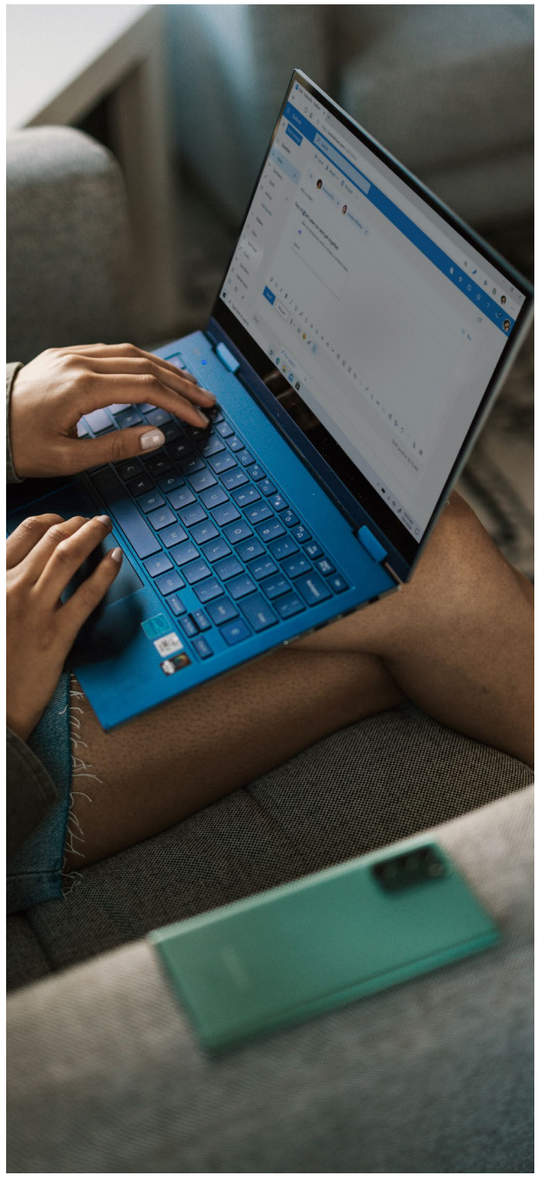
Gruppenrichtlinien

Gruppenrichtlinienname	Computer	Benutzer	WMI
All Users – Certificate Autoentrollment	Aktiviert	Aktiviert	
C-Contoso Audit	Aktiviert	Deaktiviert	
C-Contoso Proxy	Aktiviert	Aktiviert	
Computer - Allow Remote Desktop connection	Aktiviert	Deaktiviert	
Computer - Baseline security settings (W10)	Aktiviert	Deaktiviert	✓
Computer - Citrix Receiver settings	Aktiviert	Deaktiviert	
Computer - Delete Temp folder	Aktiviert	Deaktiviert	
Computer - IE11 settings	Deaktiviert	Deaktiviert	
Computer - MSOffice 2016	Aktiviert	Deaktiviert	✓
Computer - Windows 8.1 Notebook	Aktiviert	Deaktiviert	
...	...	...	

Empfohlene Maßnahmen

Gruppenrichtlinienobjekte sind in Computer-basierende und Benutzer-basierende Richtlinien geteilt, die separat verwaltet werden können. Wird ein Richtlinienanteil nicht verwendet, dann sollte der entsprechende Teil der Gruppenrichtlinie deaktiviert werden. Diese Konfigurationsänderung kann ggf. das Abrufen und die Verarbeitung von Gruppenrichtlinien während des Anmeldevorgangs beschleunigen. Unbearbeitete Gruppenrichtlinienanteile sind in der Übersicht grau hinterlegt und Anteile die schon mal bearbeitet worden sind, aber keine Client Side Extensions (CSE) mehr verknüpft haben sind mit petrol hinterlegt.

Ganzheitlich deaktivierte Gruppenrichtlinien sollten entweder nicht im Active Directory verknüpft sein oder nur kurzzeitig in diesem Zustand belassen werden, da diese erst einmal keine Funktion erfüllen. Diese Gruppenrichtlinien haben in der Übersicht beide Richtlinienanteile mit gelb hervorgehoben.



Kennzeichnet Richtlinienteile ohne Modifikation (Version = 0)

Kennzeichnet vollständig deaktivierte Richtlinien

Kennzeichnet Richtlinienteile ohne Client Side Extensions (CSE)

Konten und Rollen

Die Verwaltung bzw. Administration einer Domäne wird häufig aufgrund des hohen Aufwands auf mehrere Mitarbeiter*innen verteilt. Der AD Health Check gibt einen Gesamtüberblick, sodass z. B. veraltete Konten identifiziert werden können.

Information zu Computerkonten	
Computerkonten (insgesamt)	2381
Deaktivierte Computerkonten	9
Computerkonten mit Kerberos Unconstrained Delegation	9
Computerkonten mit Kerberos Constrained Delegation	0
Inaktive Computerkonten (Aktiviert und kein Anmeldevorgang seit 90 Tagen)	566
Aktivierte Computerkonten ohne Anmeldezeitstempel	4
Aktivierte Computerkonten, deren primäre Gruppe nicht die Domänencomputer bzw. Domänencontroller Gruppe ist	0
Computerkonten für Hyper-V virtuelle Computer	2
Computerkonten für Hyper-V Systeme	1
Computerkonten mit Windows Server Betriebssystem	178
Computerkonten mit Windows Desktop Betriebssystem	2203
Computerkonten mit anderem Betriebssystem	4
Computerkonten mit ‘unknown’ Betriebssystem	1
Computerkonten ohne Betriebssystemwert	18

Windows Server Betriebssysteme

Betriebssystem	Version	Anzahl
Windows Server 2019 Standard	10.0 (17763)	42
Windows Server 2016 Datacenter	10.0 (14393)	11
Windows Server 2016 Standard	10.0 (14393)	15
Windows Server 2012 R2 Datacenter	6.3 (9600)	8
Windows Server 2012 R2 Standard	6.3 (9600)	84
Windows Server 2008 R2 Enterprise	6.1 (7601)	3
Windows Server 2008 R2 Standard	6.1 (7601)	12
Windows Server® 2008 Standard	6.0 (6003) 6.0 (6002)	1 2

Windows Desktop Betriebssysteme

Betriebssystem	Version	Anzahl
Windows 10 Pro	10.0 (19041) - v2004 10.0 (18363) - v1909 10.0 (18362) - v1903 10.0 (17763) - v1809 10.0 (16299) - v1709 10.0 (15063) - v1703 10.0 (10586) - v1511	17 956 367 95 14 5 1
Windows 10 Enterprise	10.0 (18363) - v1909 10.0 (18362) - v1903 10.0 (16299) - v1709	10 3 1
Windows 10 Enterprise LTSC	10.0 (17763) - v1809	189
Windows 10 Enterprise 2016 LTSB	10.0 (14393) - v1607	2
Windows 10 Enterprise 2015 LTSB	10.0 (10240) - v1507	1
Windows 7 Professional	6.1 (7601)	532
Windows XP Professional	5.1 (2600)	10

Nicht auf Windows-basierende Betriebssysteme

Betriebssystem	Version	Anzahl
Mac OS X	10.6.2 (Build 10C540)	1
OnTap	NetApp Release 7.3.7P1	2
SLES	11	1

Empfohlene Maßnahmen

1. Inaktive Computerkonten, Computerkonten ohne Anmeldezeitstempel und Computerobjekte mit dem Wert „Unknown“ oder ohne Wert im Betriebssystemattribut identifizieren möglicherweise verwaiste Computerkonten im Active Directory. Aus diesem Grund sollten die entsprechenden Konten deaktiviert oder entfernt werden.

2. Alle Windows Server-basierenden Betriebssysteme vor Windows Server 2008 werden durch Microsoft nicht mehr unterstützt und Windows Server 2008 sowie 2008 R2 nur noch mit eigenen Supportverträgen. Sollten die entsprechenden Systeme nicht mehr im Einsatz ein, dann kann das identifizierte Konto auf der Domäne entfernt werden.

3. Alle Windows Desktop-basierenden Betriebssysteme vor Windows 7 und Windows 10 (v1507 - v1709; ausgenommen LTSB/LTSC Varianten) erhalten durch Microsoft keine Unterstützung mehr und Windows 7 nur noch mit separat abgeschlossenen Supportverträgen. Sollten die entsprechenden Systeme nicht mehr im Einsatz ein, dann kann das identifizierte Konto auf der Domäne entfernt werden.

Domänencontroller

Das Active Directory wird von Domänencontrollern koordiniert, die für den reibungslosen Ablauf der AD-Implementierungen unerlässlich sind. So ist der Domänencontroller der Server, der die Domäne und seine verschiedenen Objekte dezentral bereitstellt und kontrolliert.

Information zum Betriebssystem		
Allgemein	Betriebssystem	Microsoft Windows Server 2016 Standard
	Stock Keeping Unit (SKU)	7 (Server Standard Edition (full installation))
	Art der Installation	Server mit Desktopdarstellung
	Version	10.0.14393
	Service Pack	Keine
	Architektur	64-bit
	Hardwareabstraktionsschicht	Multiprocessor Free
	Verschlüsselungsstärke	256 Bit
	Installationszeitpunkt	24.07.2018 16:44:57
	Lizenzstatus	1 (Lizenziert)
Sprache	Sprache	1033 (Englisch - Vereinigte Staaten)
	Länderkode	49 (Deutschland)
	Kodetabelle	1252
	MUI Sprachpaket	en-US
Software	Microsoft .NET Framework	.NET Framework 4.6.2
	Rollen und Features (Auszug)	Active Directory-Domänendienste DNS-Server Datei- und Speicherdienste Datei- und iSCSI-Dienste Dateiserver SMB 1.0/CIFS File Sharing Support Gruppenrichtlinienverwaltung Windows PowerShell Windows PowerShell 5.1 Windows PowerShell ISE Remoteserver-Verwaltungstools WoW64-Unterstützung .NET Framework 4.6

Arbeitsspeicher

Speicherauslastung (Momentaufnahme)		
Memory	Gesamter physischer Speicher	7,99 GB
	Verfügbarer physischer Speicher	4,97 GB
	Gesamter virtueller Speicher	9,24 GB
	Verfügbarer virtueller Speicher	6,09 GB
	Verfügbarer Speicher in Auslagerungsdatei	0,92 GB
Pagefile	Auslagerungsdatei	C:\pagefile.sys
	Anfangsgröße	1.280 MB
	Zurzeit verwendet	132 MB
	Zwischenzeitlich max. verwendet	401 MB

Empfohlene Maßnahmen

1. Das .NET Framework 4.6.2, welches im Lieferumfang von Windows Server 2016 enthalten ist, wird per Microsoft Update nicht mehr mit Sicherheitsaktualisierungen versorgt, sondern ausschließlich das .NET Framework 4.8. Aus diesem Grund sollte das .NET Framework 4.8 auf diesem System nachinstalliert werden, um so die aktuellen Sicherheitsaktualisierungen zu erhalten.

2. Das Feature „SMB 1.0/CIFS File Sharing Support" stellt das originale SMB Protokoll für den Zugriff auf Freigaben bereit und wird in den neusten Windows-Versionen standardmäßig nicht mehr zur Verfügung gestellt. Das entfernen dieses Merkmals würde Betriebssysteme vor Windows Vista bzw. Windows Server 2008 sowie nicht-Windows-basierende Betriebssysteme ohne SMBv2 Unterstützung den Zugriff auf freigegebene Ordner auf den Domänencontrollern verweigern. D.h. die betroffenen Systeme können nicht mehr die Freigabe „Netlogon" aufrufen, keine Gruppenrichtlinien mehr verarbeiten und ggf. keinen Zugriff auf Domänen-basierte DFS-Stammordner erhalten. Sind die entsprechenden Rahmenbedingungen erfüllt sollte zur Erhöhung der Sicherheitskonfiguration dieses Merkmal von den Domänencontrollern entfernt werden. Auf der anderen Seite muss das Feature auf den Windows Server 2019-basierenden Domänencontrollern nachinstalliert werden, wenn noch ältere Betriebssysteme unterstützt werden müssen.

3. (Optional) Ein Domänencontroller kann in den aktuellen Microsoft Windows Betriebssystemen mit oder ohne grafische Oberfläche betrieben werden. Seit Windows Server 2016 kann die Auswahl nach der Erstinstallation nicht mehr verändert werden. Die sogenannte Server Core Variante benötigt bedingt durch ihre Größe einen geringeren Ressourcenbedarf und bietet durch fehlende Komponenten eine geringere Angriffsfläche. Auf der anderen Seite sollte im Vorfeld eines Betriebs verifiziert werden, ob alle eigensetzten System Management Produkte auch auf einem System ohne grafische Oberfläche installiert und betrieben werden können, damit der Server Core in Zukunft als Domänencontroller verwendet werden kann.

Microsoft DNS-Dienst

DNS ist das Namensauflösungsprotokoll für TCP/IP-Netzwerke. Als wesentlicher Bestandteil des Internets ermöglicht es die Nutzung einfach zu merkender alphanumerischer URLs statt kryptischer IP-Adressen. So stellen der DNS-Client und DNS-Server Computername-zu-IP-Adress-Übersetzung für Computer und Benutzer bereit. Wenn Sie eine neue Domänenstruktur installieren, können Sie den Microsoft DNS-Dienst automatisiert mit installieren oder einen vorhanden Dienst im Netzwerk nutzen.

Active Directory-integrierte Zonen

DC=ForestDnsZones, DC=contoso, DC=com

Forward-/Reverse-Lookupzonen und Vertrauenspunkte

DNS-Lookupzonen	Zonentyp	Dynamische Updates	Zonenalterung / Aufräumvorgang
TrustAnchors	Primär	Keine	Deaktiviert

Bedingte Weiterleitungen

DNS-Lookupzonen	Zonentyp	Masterservers
fabrikam.com	Bedingte Weiterleitung	172.10.250.1

DC=DomainDnsZones, DC=contoso, DC=com

Forward-/Reverse-Lookupzonen und Vertrauenspunkte

DNS-Lookupzonen	Zonentyp	Dynamische Updates	Zonenalterung / Aufräumvorgang
250.169.10.in-addr.arpa	Primär	Keine	Deaktiviert
contoso.com	Primär	Nur sichere	Deaktiviert
northwindtraders.com	Stub	Nur sichere	Deaktiviert

DC=contoso, DC=com

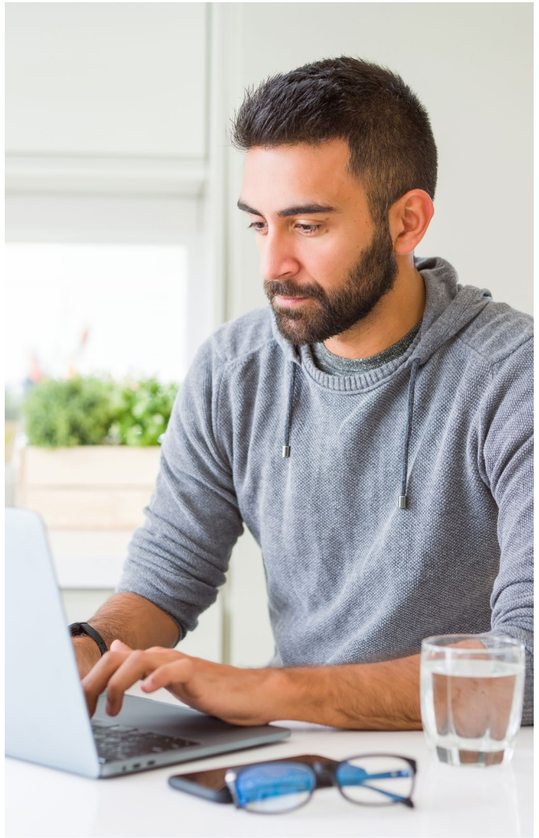
Forward-/Reverse-Lookupzonen und Vertrauenspunkte

DNS-Lookupzonen	Zonentyp	Dynamische Updates	Zonenalterung / Aufräumvorgang
68.10.in-addr.arpa	Primär	Nur sichere	Deaktiviert
69.10.in-addr.arpa	Primär	Nur sichere	Deaktiviert
69.172.in-addr.arpa	Primär	Nur sichere	Deaktiviert
200.69.172.in-addr.arpa	Primär	Nicht sichere und sichere	Deaktiviert
am.contoso.com	Primär	Nur sichere	Deaktiviert
contoso.net	Primär	Nur sichere	Deaktiviert

Empfohlene Maßnahmen

(Optional) Mit der Einführung von Anwendungspartitionen für den DNS-Dienst wurden die DNS-Zonen nicht mehr in der Domänenpartition gespeichert, sondern in den explizit für den DNS-Dienst angelegten Anwendungspartitionen ForestDnsZones und DomainDnsZones.

Darüber hinaus ist es weiterhin noch möglich eine DNS-Zone in der Domänenpartition abzulegen. Um dem aktuellen Standard zu entsprechen können die DNS-Zonen, die aktuell im Namenkontext DC=contoso,DC=com gespeichert sind, in die entsprechenden Anwendungspartitionen umgezogen werden.



Lassen Sie Ihre AD Domain Services regelmäßig überprüfen

Das Active Directory stets fehlerfrei zu halten, ist von entscheidender Bedeutung. Denn Probleme wirken sich schnell negativ auf die Sicherheit, Leistung, Verfügbarkeit und Produktivität aus.

Sie möchten einen Active Directory Domain Services Health Check durchführen und die Basis für gesunde Prozesse schaffen? Kontaktieren Sie uns und lassen Sie sich von unseren Experten auf Augenhöhe beraten.

novaCapta

Ihr Microsoft Premium Partner

Kontaktieren Sie uns!

Bei Fragen zu unseren Themen sind wir gerne für Sie da und finden gemeinsam mit Ihnen die beste Auswahl aus den Microsoft Bausteinen

DE

novaCapta GmbH
Im Mediapark 5c
50670 Köln

T +49 (0)221 58919 343
M info@novacapta.com
W www.novacapta.com

CH

novaCapta Schweiz AG
Industriestrasse 5a
6210 Sursee

T +41 (0)41 392 20 00
M info.schweiz@novacapta.com
W www.novacapta.ch