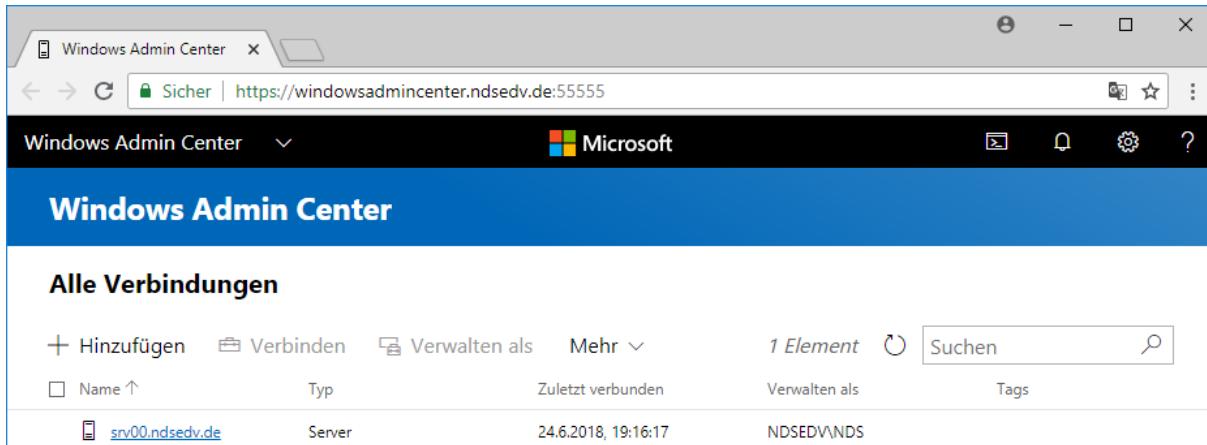




Windows Admin Center – Honolulu installieren

Das Windows Admin Center ist eine komplette Neuentwicklung zur zentralisierten Administration von Windows Servern. Das WAC setzt auf Powershell und deren Fähigkeiten, Server per WMI und WS-Management-Schnittstellen zugänglich zu machen.



In diesem Dokument gehe ich auf die Installation ein und zeige euch, was alles eingerichtet werden muss, um das WAC sicher betreiben zu können.

Die Installation setzt als Basis ein Windows 10 v1709 (Desktop-Betrieb) oder Windows Server 2016 (Gateway-Betrieb) voraus. Damit sich ein Server über das WAC remote verwalten lässt, muss die Funktion zunächst auf dem/den Zielserver(n) aktiviert werden. In einer Domäne setzen wir natürlich auf Gruppenrichtlinien.

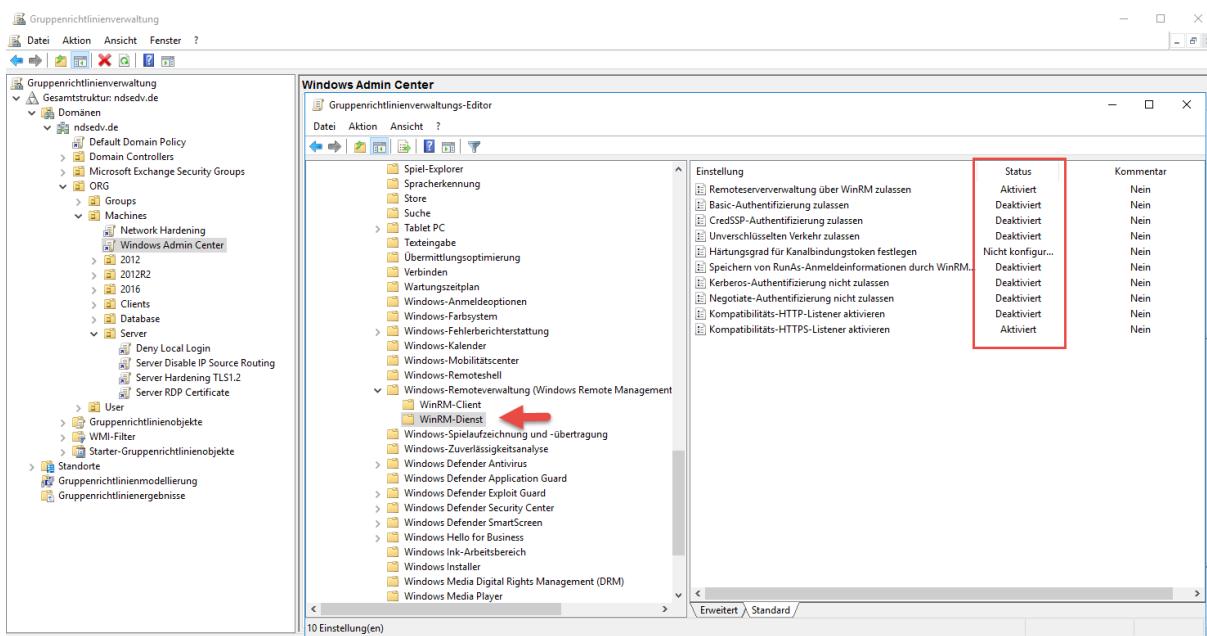
Vorbereitungen:

Als erstes legen wir ein neues GRO an und konfigurieren damit unsere Server- oder/und Client-Systeme.

Windows Remote Management-Dienst aktivieren:

Die beiden Richtlinien sind das Minimum, alle anderen erhöhen zusätzlich die Sicherheit.

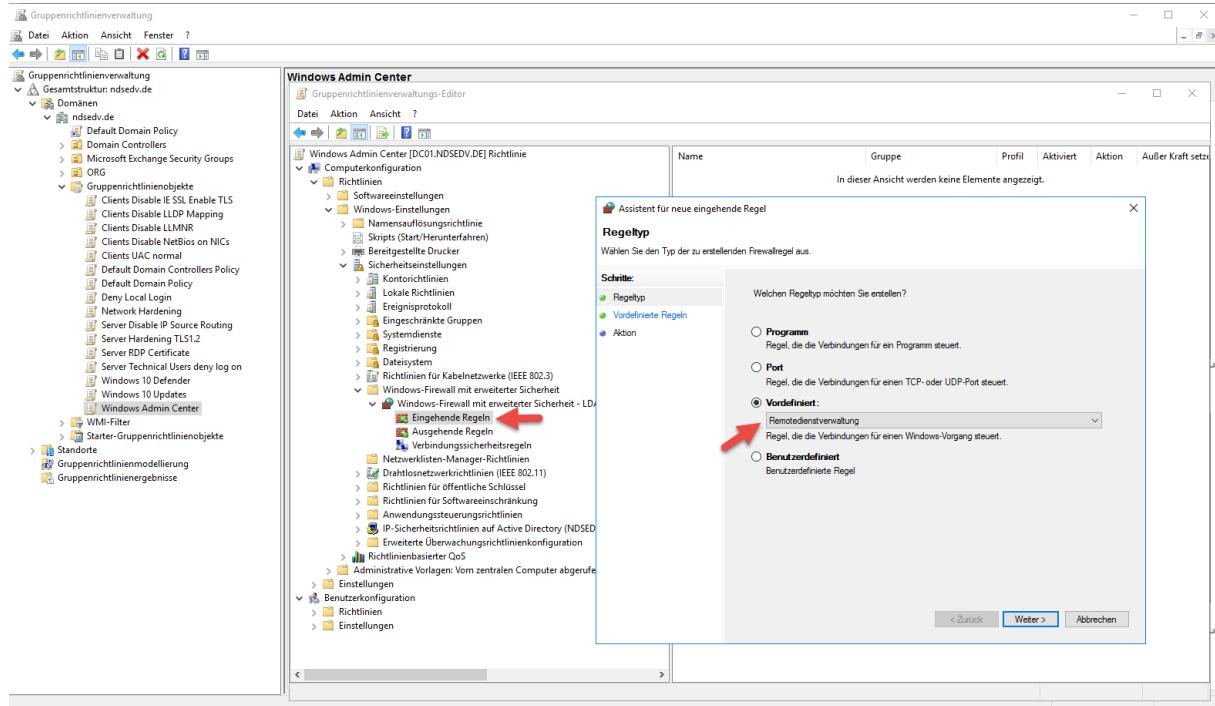
- WinRM Dienst und den HTTPS Listener aktivieren



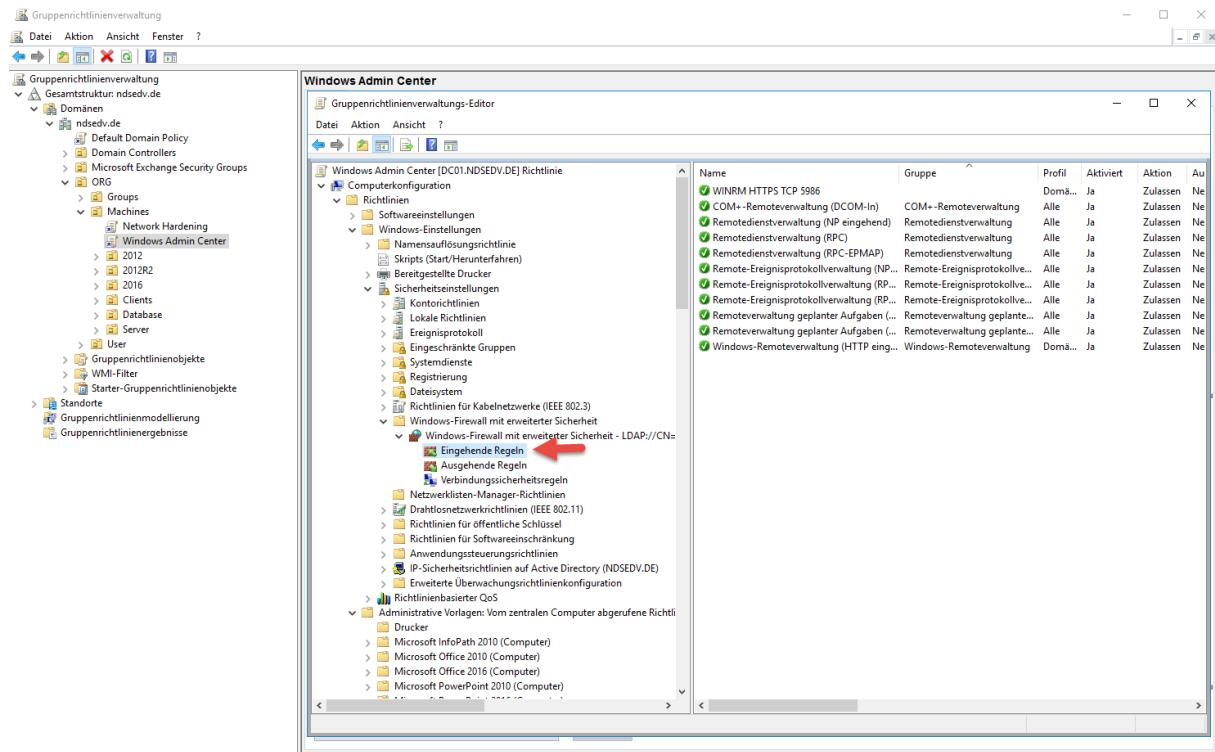


Windows Admin Center – Honolulu installieren

Firewall Regeln konfigurieren:



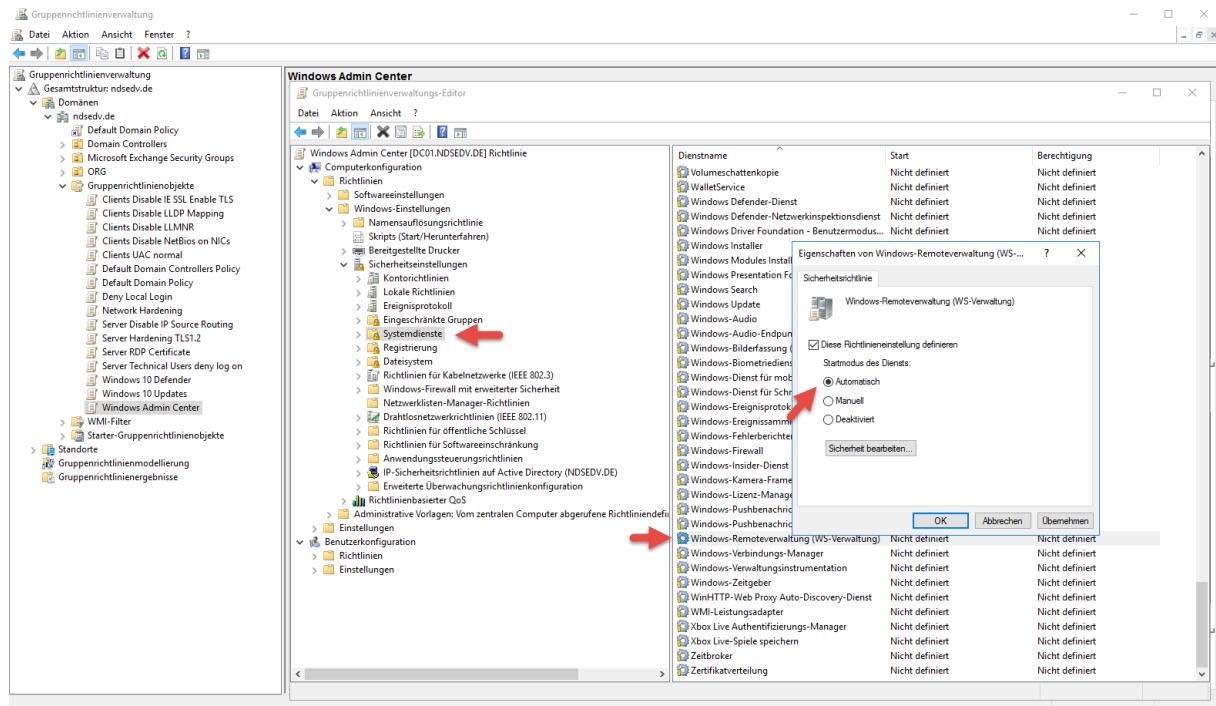
Zur Vervollständigung aktiviere ich diese ganzen Regeln.



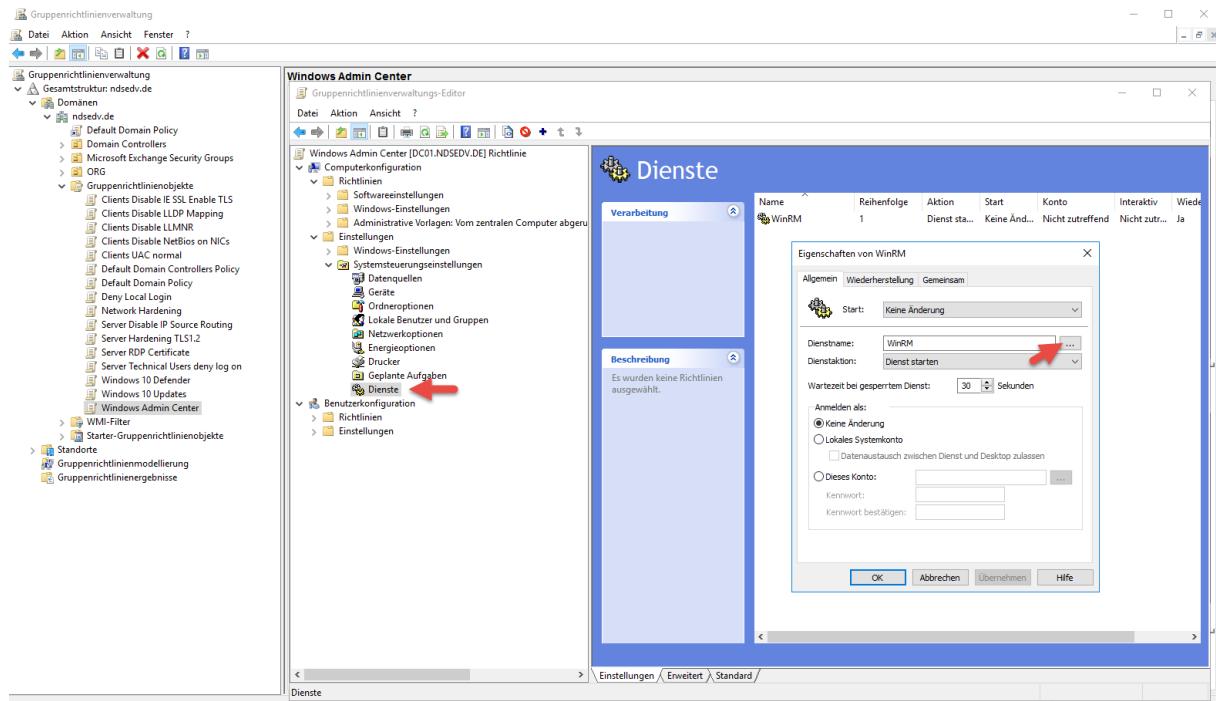


Windows Admin Center – Honolulu installieren

Systemdienst - Windows-Remoteverwaltung (WS-Verwaltung) konfigurieren:



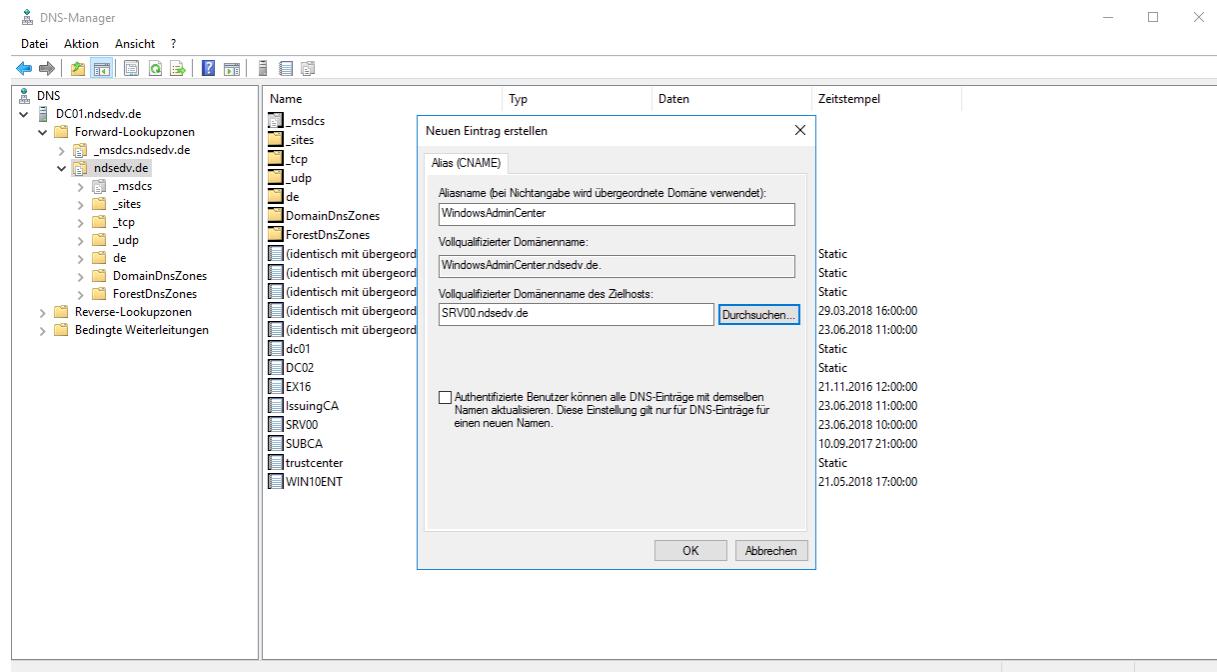
Den Dienst WinRM individuell konfigurieren:



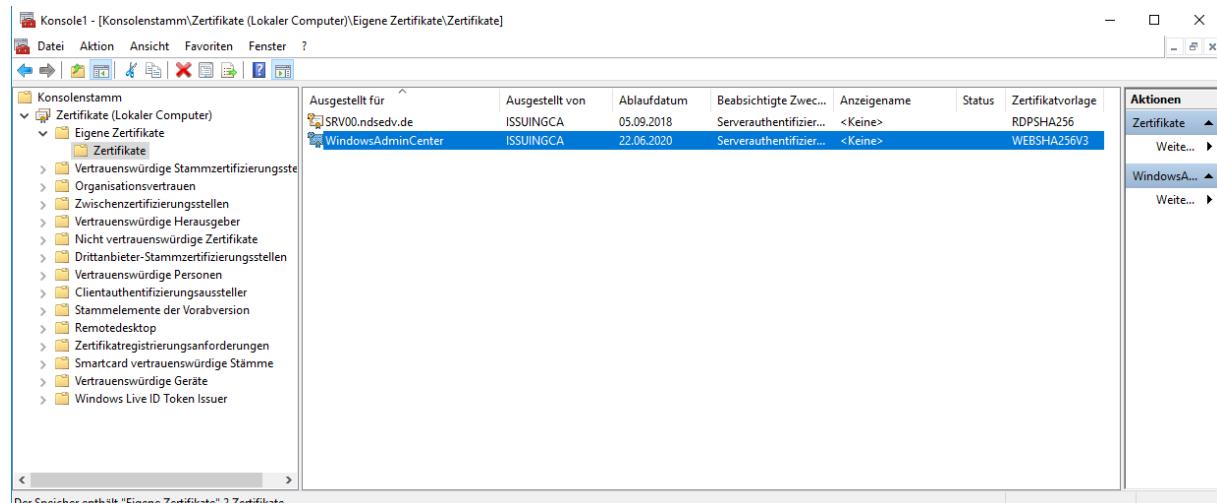


Windows Admin Center – Honolulu installieren

CNAME mit Verweis auf den Gateway-Server erstellen (Name des Zertifikats):



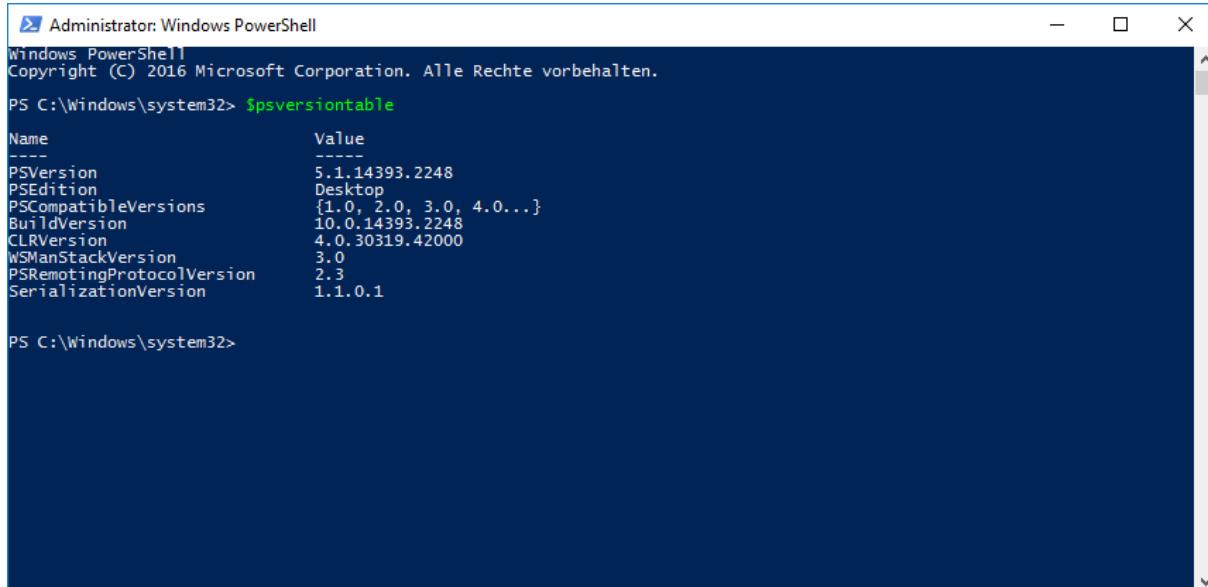
Zertifikat für den Gateway-Server auf dem Server SRV00 beantragen:





Windows Admin Center – Honolulu installieren

Powershell Version abfragen ggfls. updaten ([ab 5.1](#)):



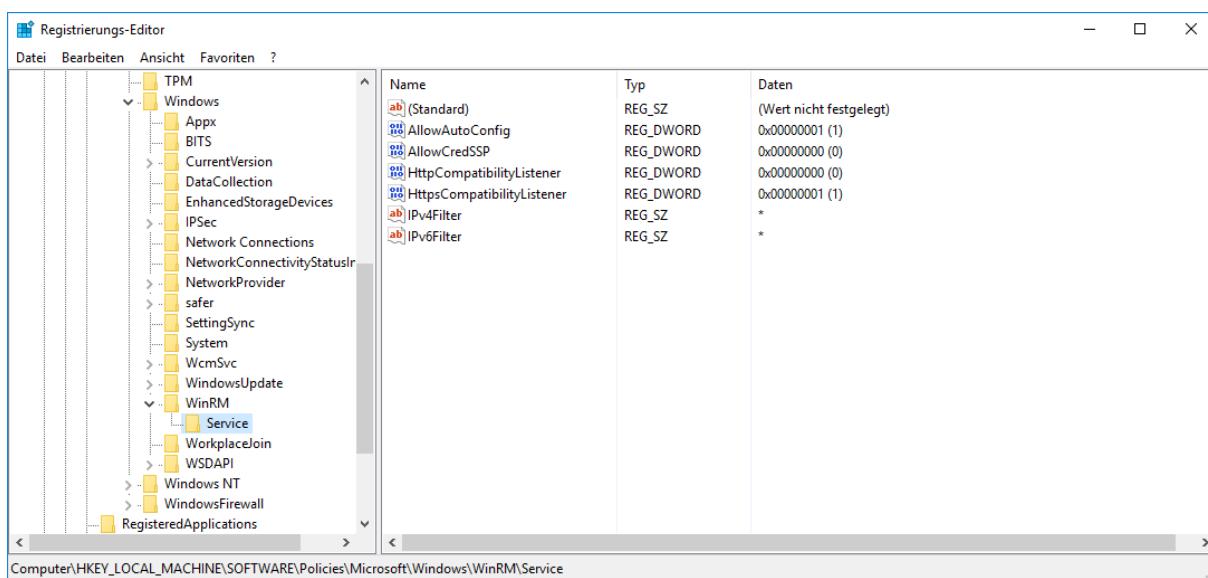
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Windows\system32> $psversiontable

Name           Value
----           -----
PSVersion      5.1.14393.2248
PSEdition      Desktop
PSCompatibleVersions {1.0, 2.0, 3.0, 4.0...}
BuildVersion   10.0.14393.2248
CLRVersion     4.0.30319.42000
WSManStackVersion 3.0
PSRemotingProtocolVersion 2.3
SerializationVersion 1.1.0.1

PS C:\Windows\system32>
```

Die angewendete Gruppenrichtlinie zum WinRMService finden wir in der Registry an dieser Stelle:



Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
AllowAutoConfig	REG_DWORD	0x00000001 (1)
AllowCredSSP	REG_DWORD	0x00000000 (0)
HttpCompatibilityListener	REG_DWORD	0x00000000 (0)
HttpsCompatibilityListener	REG_DWORD	0x00000001 (1)
IPv4Filter	REG_SZ	*
IPv6Filter	REG_SZ	*



Windows Admin Center – Honolulu installieren

Installation und Einrichtung:

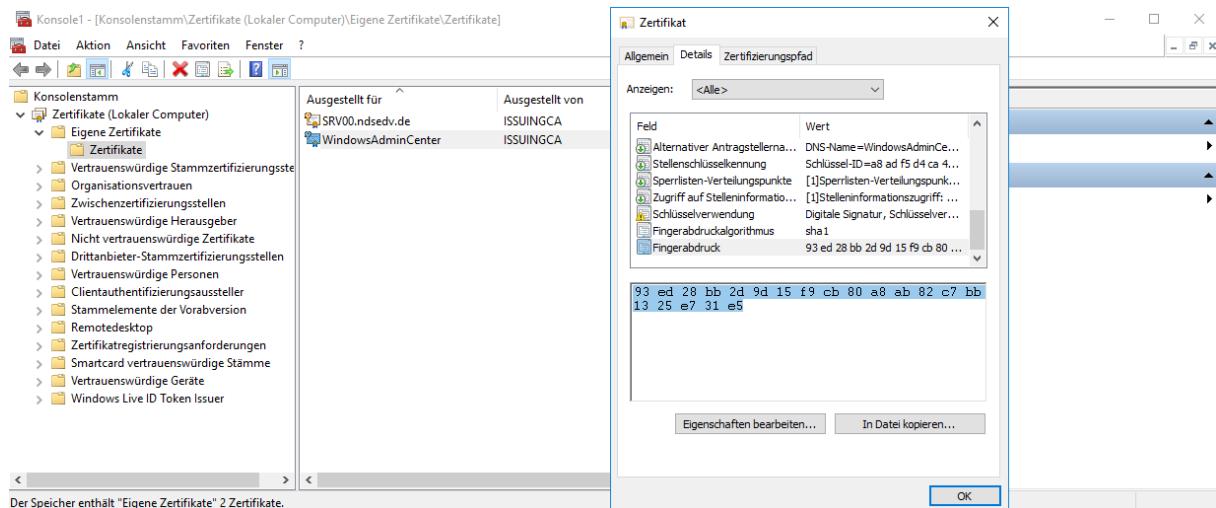
[Download-Link](#)



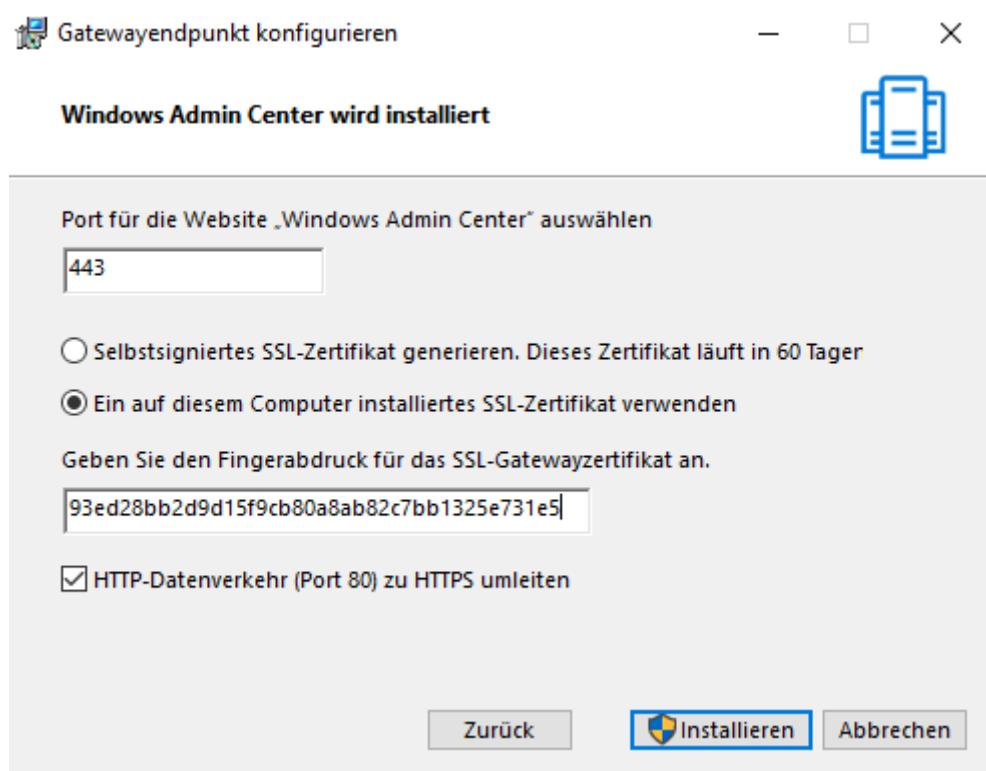


Windows Admin Center – Honolulu installieren

Fingerprint des Zertifikats ermitteln und kopieren:



Port bestimmen (8129) und Fingerprint für das SSL Zertifikat einfügen:

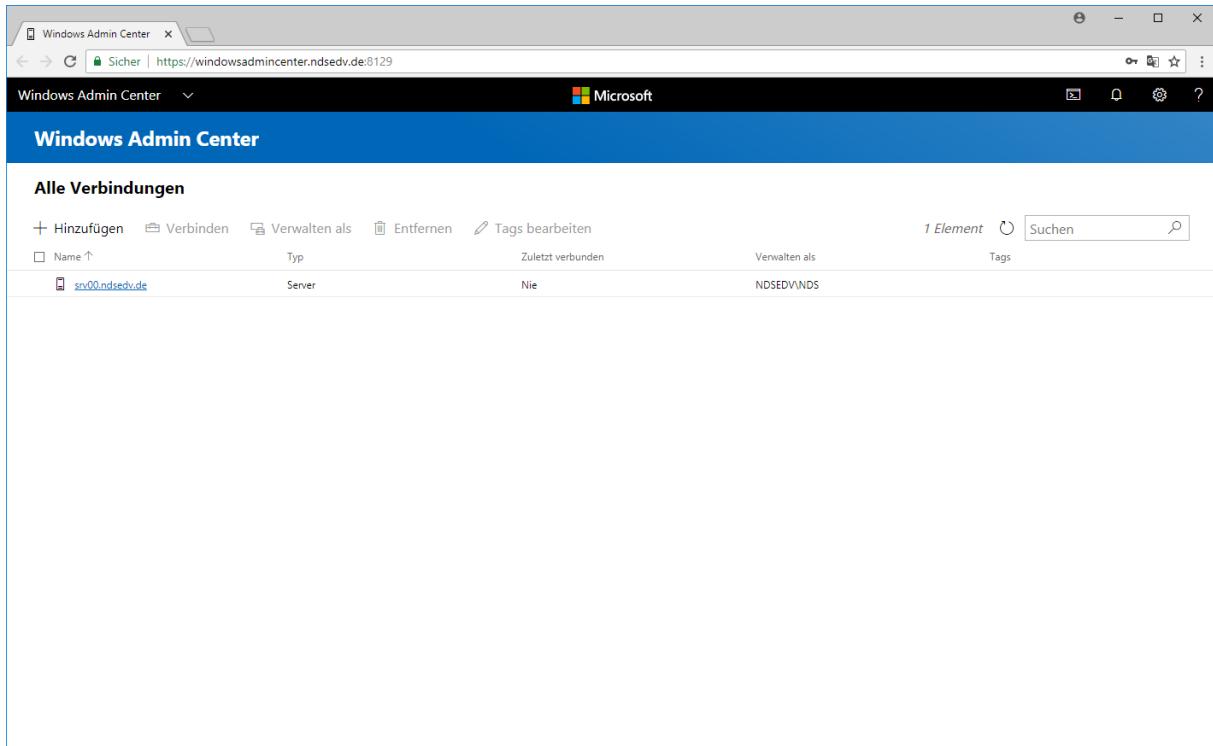


Die Installation ist abgeschlossen!

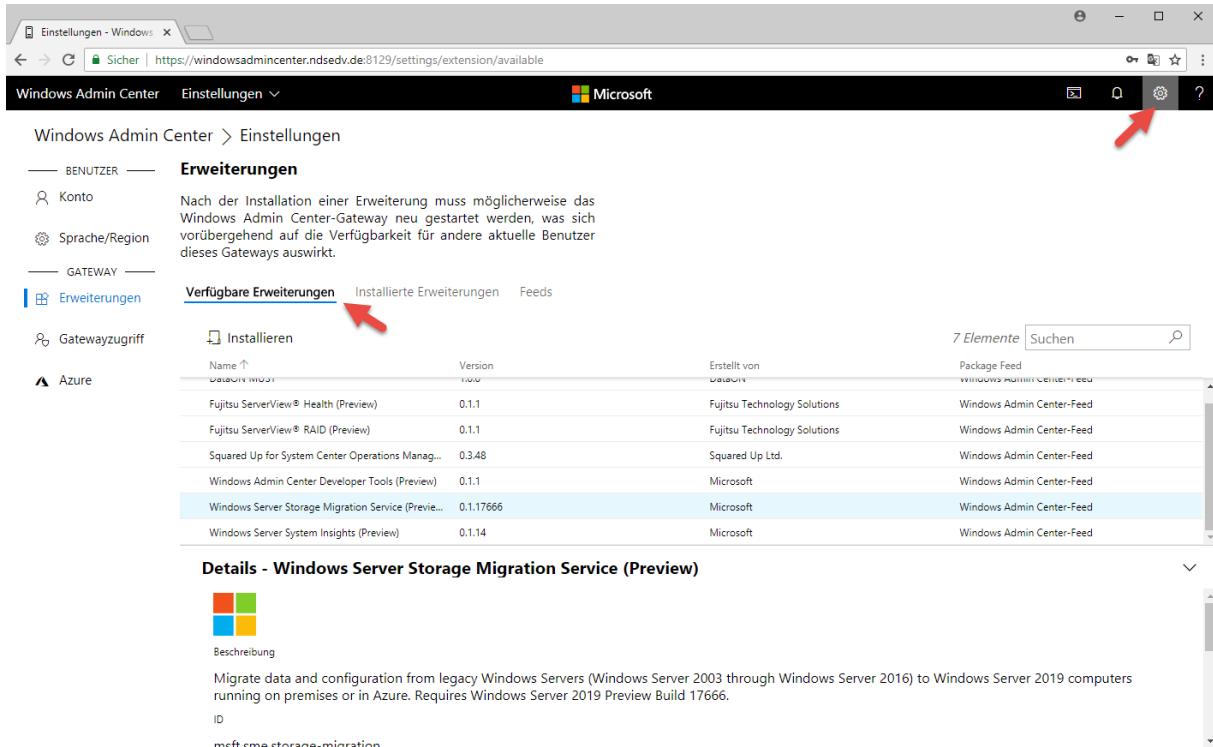


Windows Admin Center – Honolulu installieren

Erster Start des Windows Admin Centers:



Erweiterungen herunterladen, wenn notwendig:



Windows Admin Center > Einstellungen

Erweiterungen

Nach der Installation einer Erweiterung muss möglicherweise das Windows Admin Center-Gateway neu gestartet werden, was sich vorübergehend auf die Verfügbarkeit für andere aktuelle Benutzer dieses Gateways auswirkt.

Verfügbare Erweiterungen [Installierte Erweiterungen](#) [Feeds](#)

Details - Windows Server Storage Migration Service (Preview)

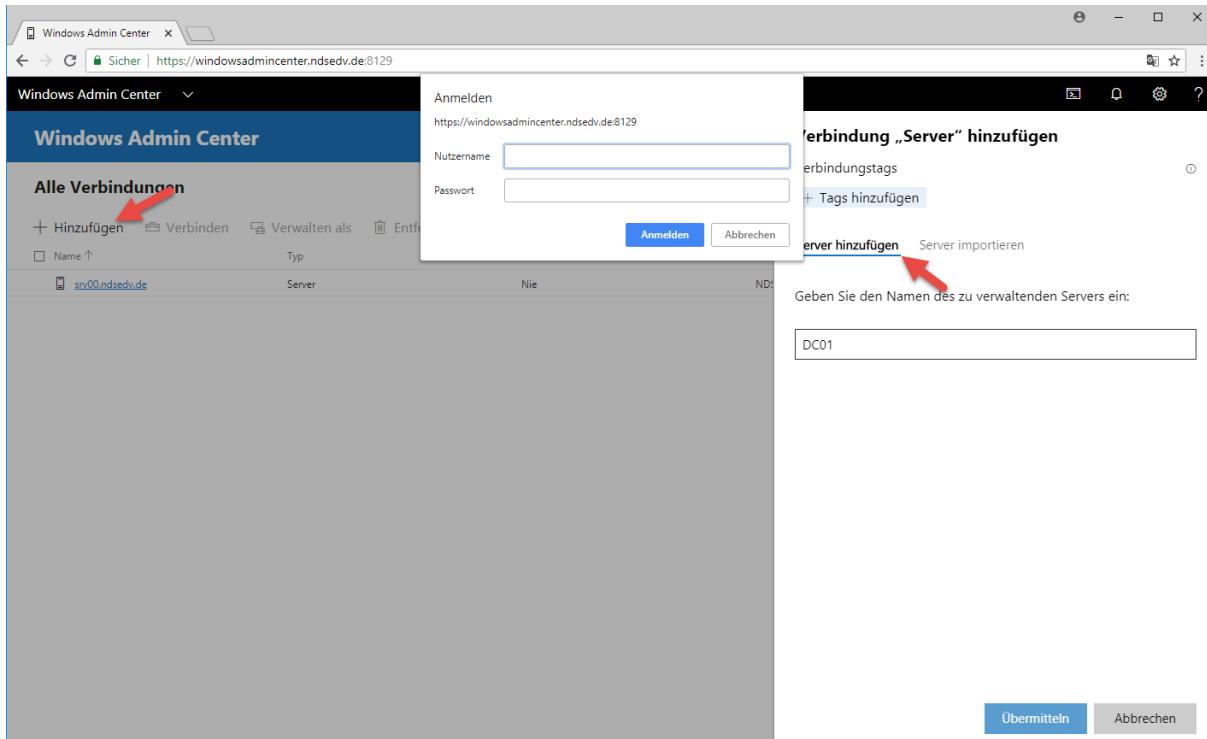
Beschreibung
Migrate data and configuration from legacy Windows Servers (Windows Server 2003 through Windows Server 2016) to Windows Server 2019 computers running on premises or in Azure. Requires Windows Server 2019 Preview Build 17666.

ID
microsoft/Windows-Storage-Migration

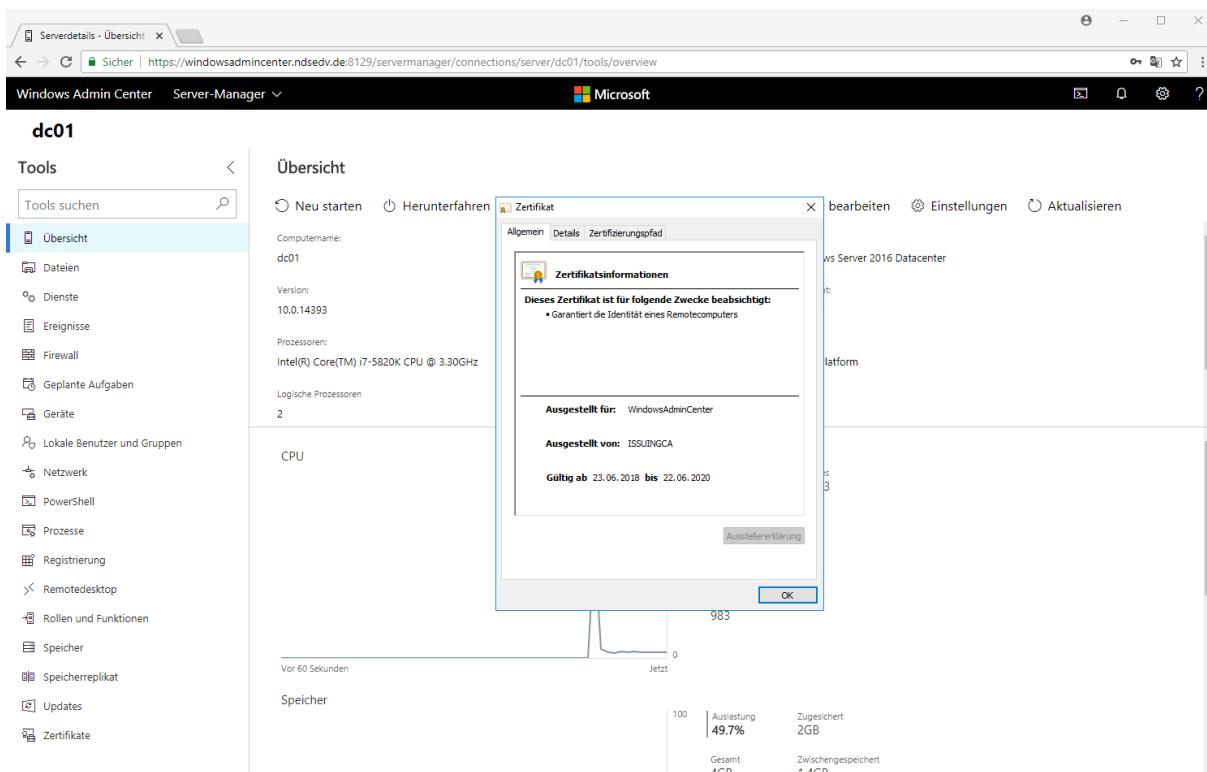


Windows Admin Center – Honolulu installieren

Ziel-Server zum Administrieren hinzufügen:



An dieser Stelle können wir gerne noch einmal das eingesetzte Zertifikat kontrollieren:



Das WAC nutzt zur Verbindung und Verwaltung die standardmäßigen Windows Server Tools wie die Remoteverwaltung, WMI oder eine Powershell Remotesitzung.



Windows Admin Center – Honolulu installieren

Ab hier zeige ich ein paar Bilder was alles administriert werden und welche Informationen man sich anzeigen lassen kann.

Übersicht:

Übersicht

dc01

Tools

- Übersicht
- Dateien
- Dienste
- Ereignisse
- Firewall
- Geplante Aufgaben
- Geräte
- Lokale Benutzer und Gruppen
- Netzwerk
- PowerShell
- Prozesse
- Registrierung
- Remotedesktop
- Rollen und Funktionen
- Speicher
- Speicherreplikat
- Updates
- Zertifikate

Übersicht

Computername: dc01 Domäne: ndsedv.de Betriebssystem: Microsoft Windows Server 2016 Datacenter

Version: 10.0.14393 Installierter Speicher (RAM): 4 GB Speicherplatz gesamt: 60.09 GB

Prozessoren: Intel(R) Core(TM) i7-5820K CPU @ 3.30GHz Hersteller: VMware, Inc. Modell: VMware Virtual Platform

Logische Prozessoren: 2 Freier Speicherplatz: 37.07 GB NIC(s): 1

Betriebszeit: 0:14:02 Anzahl der Benutzer: 1

CPU

Auslastung: 39% Handles: 31823

Geschwindigkeit: 3.37GHz Prozesse: 60

Threads: 900

Vor 60 Sekunden Jetzt

Speicher

Auslastung: 100% Zugewichtet

Dateien:

Übersicht

Dateien

Neuer Ordner Löschen Mehr

Name	Geändert am	Typ	Größe
VMware Tools (D:)		Volume	100.928 KB
(C:)		Volume	62.912.508 KB



Windows Admin Center – Honolulu installieren

Dienste:

Name	Anzeigename	Status	Startmodus
ADWS	Active Directory-Webdienste	Running	Automatic
AIRouter	AllJoyn-Routerdienst	Stopped	Manual (Triggered)
ALG	Gatewaydienst auf Anwendungsebene	Stopped	Manual
AppIDSvc	Anwendungsidentität	Stopped	Manual (Triggered)
AppInfo	Anwendungsinformationen	Running	Manual (Triggered)
AppMgmt	Anwendungsverwaltung	Stopped	Manual
AppReadiness	App-Vorbereitung	Stopped	Manual
AppVClient	Microsoft App-V Client	Stopped	Disabled
AppXSvc	AppX-Bereitstellungsdienst (AppXSVC)	Stopped	Manual
AudioEndpointBuilder	Windows-Audio-Endpunktberstellung	Stopped	Manual
Audiosrv	Windows-Audio	Stopped	Manual
AxInstSV	ActiveX-Installer (AxInstSV)	Stopped	Manual
BFE	Basisfiltermodul	Running	Automatic
BITS	Intelligenter Hintergrundübertragungsdienst	Stopped	Manual

Ereignisse:

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID
Informationen	23.6.2018, 11:31:45	Windows Error Reporting	1001
Informationen	23.6.2018, 11:31:45	Windows Error Reporting	1001
Fehler	23.6.2018, 11:31:44	Application Error	1000
Informationen	23.6.2018, 11:16:42	.NET Runtime Optimization Service	1130
Informationen	23.6.2018, 11:11:27	Microsoft-Windows-LoadPerf	1000
Fehler	23.6.2018, 11:11:27	Microsoft-Windows-PerfNet	2006
Informationen	23.6.2018, 11:08:19	ESENT	326
Informationen	23.6.2018, 11:08:19	ESENT	105
Informationen	23.6.2018, 11:08:19	ESENT	102
Informationen	23.6.2018, 11:06:06	VSS	8224
Informationen	23.6.2018, 11:05:36	Microsoft-Windows-Security-SPP	903
Informationen	23.6.2018, 11:05:36	Microsoft-Windows-Security-SPP	16384
Fehler	23.6.2018, 11:05:27	Microsoft-Windows-PerfNet	2006
Fehler	23.6.2018, 11:05:27	Microsoft-Windows-PerfNet	2006
Informationen	23.6.2018, 11:05:06	Microsoft-Windows-Security-SPP	902
Informationen	23.6.2018, 11:05:06	Microsoft-Windows-Security-SPP	1003
Informationen	23.6.2018, 11:05:06	Microsoft-Windows-Security-SPP	1066
Informationen	23.6.2018, 11:05:06	Microsoft-Windows-Security-SPP	900
Informationen	23.6.2018, 11:04:35	Microsoft-Windows-Security-SPP	903
Informationen	23.6.2018, 11:04:35	Microsoft-Windows-Security-SPP	16384



Windows Admin Center – Honolulu installieren

Firewall:

The screenshot shows the Windows Admin Center interface for the server 'dc01'. The left sidebar is the 'Tools' menu, with 'Firewall' selected. The main content area is titled 'Firewall' and shows the 'Übersicht' (Overview) tab. It displays three connection profiles: 'Domain' (Aktiviert), 'Private' (Aktiviert), and 'Public' (Aktiviert). For each profile, the 'Standardaktion für Eingehende' (Incoming standard action) is 'Blockieren' and the 'Standardaktion für Ausgehende' (Outgoing standard action) is 'Zulassen' (Allow). The URL in the browser is <https://windowsadmincenter.ndsedv.de:8129/servermanager/connections/server/dc01/tools/firewall>.

Geplante Aufgaben:

The screenshot shows the Windows Admin Center interface for the server 'dc01'. The left sidebar is the 'Tools' menu, with 'Geplante Aufgaben' selected. The main content area is titled 'Geplante Aufgaben' (Scheduled Tasks) and shows a list of four tasks in the 'Aufgabenplanungsbibliothek' (Task Scheduler Library). The tasks are: 'CreateExplorer...', 'User_Feed_Syn...', 'User_Feed_Syn...', and 'User_Feed_Syn...'. The table includes columns for Name, Status, Trigger, Zeit der nächsten Ausführung (Next run time), Zeit der letzten Ausführung (Last run time), Ergebnis der letzten Ausführung (Last run result), Autor (Owner), and Erstellt (Created). The URL in the browser is <https://windowsadmincenter.ndsedv.de:8129/servermanager/connections/server/dc01/tools/scheduledtasks>.



Windows Admin Center – Honolulu installieren

Geräte:

Geräte

174 Elemente

Suchen

Name	Status
Anschlüsse (COM und LPT)	
Audio-, Video- und Gamecontroller	
Batterien	
Computer	
Druckerwarteschlangen	
DVD-/CD-ROM-Laufwerke	
Eingabegeräte (Human Interface Devices)	
Grafikkarten	
IDE ATA/ATAPI-Controller	
Laufwerke	
Monitore	
Mäuse und andere Zeigegeräte	
Netzwerkadapter	
Prozessoren	
Softwaregeräte	
Speichercontroller	
Speichernolumes	
Systemgeräte	
Tastaturen	
USB-Controller	

Netzwerk:

Einstellungen

Name	Beschreibung	Status	IPv4-Adresse	IPv6-Adresse
Ethernet0	Intel(R) 82574L Gigabit Network Connection	Up	172.18.32.31	

Details

Name	Beschreibung	NIC-Index
Ethernet0	Intel(R) 82574L Gigabit Network Connection	2

Status	MAC-Adresse	Übertragungsrate
Up	00-0C-29-FA-19-78	1 Gbps

IPv4-Adresse	Sekundäre IPv4-Adresse	IPv4-Präfixlänge
172.18.32.31	Keine konfiguriert	24

IPv4-Standardgateway	IPv4-DHCP	IPv4-DNS-Server
172.18.32.1	Nein	127.0.0.1 172.18.32.31

IPv6-Adresse	Verbindungslokale IPv6-Adresse	Sekundäre IPv6-Adresse
Keine konfiguriert	Keine konfiguriert	Keine konfiguriert

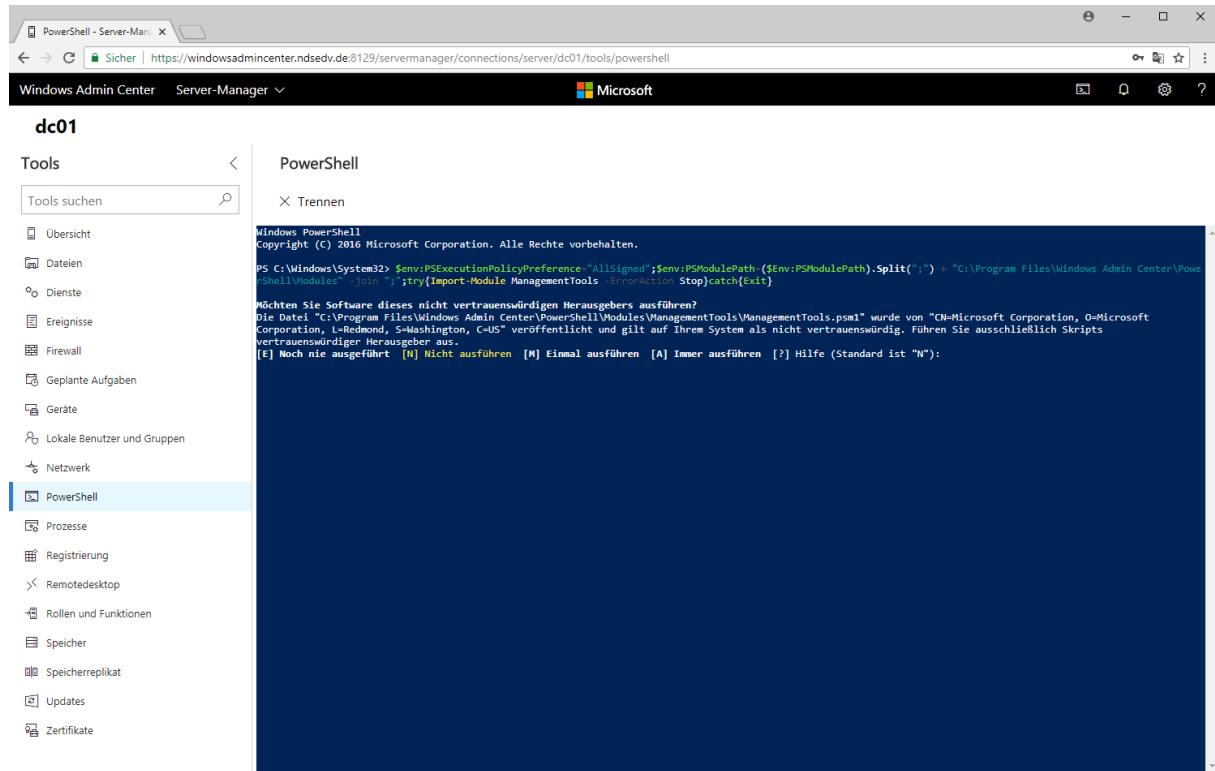
IPv6-Präfixlänge	IPv6-Standard-Gateway	IPv6-DHCP
Keine konfiguriert	Keine konfiguriert	Nein

IPv6-DNS-Server	Keine konfiguriert
Keine konfiguriert	



Windows Admin Center – Honolulu installieren

Powershell:

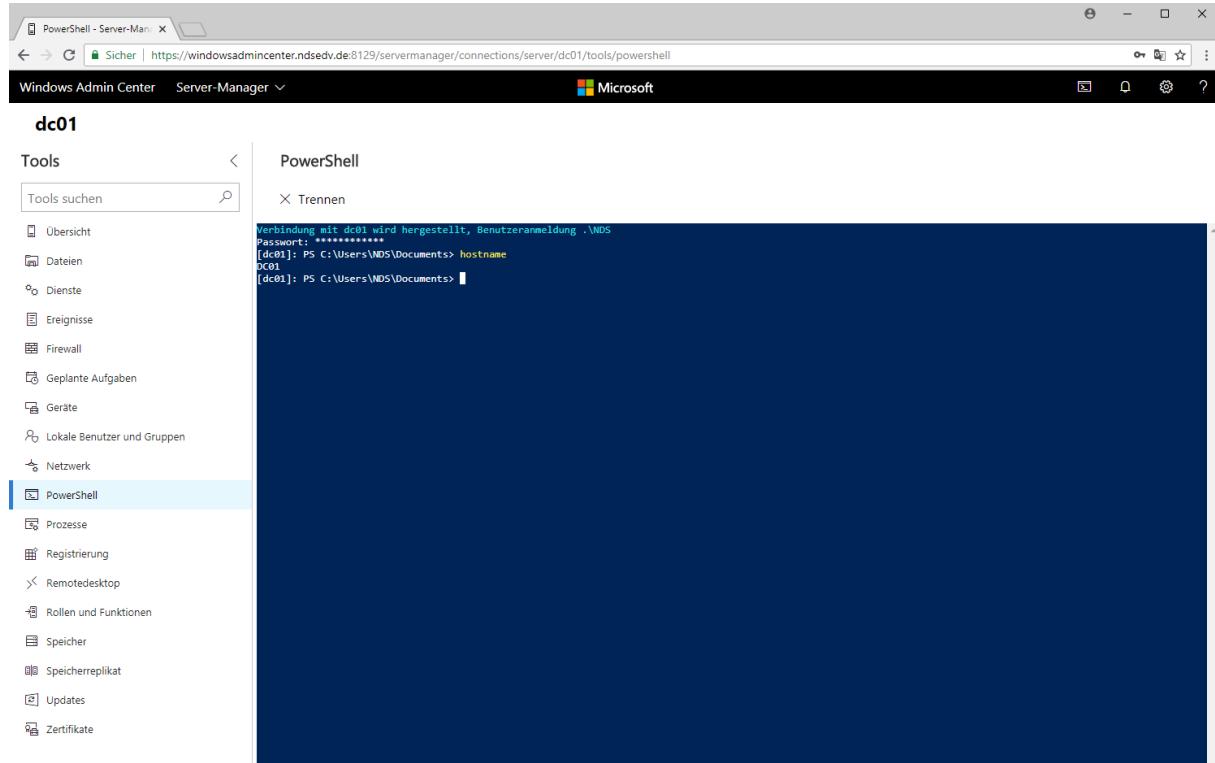


```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Windows\System32> $env:PSExecutionPolicyPreference="AllSigned";$env:PSModulePath=($env:PSModulePath).Split(',') + "C:\Program Files\Windows Admin Center\PowerShell\Modules" -join ";";try{Import-Module ManagementTools -ErrorAction Stop}catch{Exit}

Möchten Sie Software dieses nicht vertrauenswürdigen Herausgebers ausführen?
Die Datei "C:\Program Files\Windows Admin Center\PowerShell\Modules\ManagementTools.psm1" wurde von "CN=Microsoft Corporation, O=Microsoft Corporation, L=Redmond, S=Washington, C=US" veröffentlicht und gilt auf Ihrem System als nicht vertrauenswürdig. Führen Sie ausschließlich Skripts vertrauenswürdiger Herausgeber aus.
[E] Noch nie ausgeführt [N] Nicht ausführen [M] Einmal ausführen [A] Immer ausführen [?] Hilfe (Standard ist "N"):
```

Einfach nur genial!



```
Verbindung mit dc01 wird hergestellt, Benutzeranmeldung .\NDS
Passwort: ****
[dc01]: PS C:\Users\NDS\Documents> hostname
DC01
[dc01]: PS C:\Users\NDS\Documents> [
```



Windows Admin Center – Honolulu installieren

Prozesse:

The screenshot shows the Windows Admin Center interface for the server 'dc01'. The left sidebar is titled 'Tools' and lists various management options. The 'Prozesse' (Processes) tool is selected and active. The main pane displays a table of 64 running processes. The columns are: Name, PID, Status, CPU, Benutzername (Username), and Arbeitssatz (Arbeitsspeich..) (Working Set (Working Set)). The table includes entries for system processes like 'Leerlaufprozess', 'Systeminterrupts', 'System', and various 'svchost.exe' and 'services.exe' processes, along with other system and network-related services.

Name	PID	Status	CPU	Benutzername	Arbeitssatz (Arbeitsspeich..)
Leerlaufprozess	0	Wird ausgeführt...	49.9 %	SYSTEM	4 KB
Systeminterrupts	1	Wird ausgeführt...	0 %	SYSTEM	0 B
System	4	Wird ausgeführt...	0 %	SYSTEM	136 KB
smss.exe	384	Wird ausgeführt...	0 %	SYSTEM	1.21 MB
csrss.exe	476	Wird ausgeführt...	0 %	SYSTEM	4.24 MB
csrss.exe	548	Wird ausgeführt...	0 %	SYSTEM	5.28 MB
wininit.exe	556	Wird ausgeführt...	0 %	SYSTEM	4.69 MB
winlogon.exe	624	Wird ausgeführt...	0 %	SYSTEM	8.77 MB
svchost.exe	668	Wird ausgeführt...	0 %	Netzwerkdienst	11.3 MB
services.exe	672	Wird ausgeführt...	0 %	SYSTEM	9.57 MB
lsass.exe	680	Wird ausgeführt...	0 %	SYSTEM	94.8 MB
svchost.exe	788	Wird ausgeführt...	0 %	Lokaler Dienst	27.49 MB
dllhost.exe	816	Wird ausgeführt...	0 %	SYSTEM	12.12 MB
svchost.exe	848	Wird ausgeführt...	0 %	SYSTEM	19.2 MB
svchost.exe	900	Wird ausgeführt...	0 %	Netzwerkdienst	11.13 MB
svchost.exe	1000	Wird ausgeführt...	0 %	Lokaler Dienst	24.57 MB
dwm.exe	1020	Wird ausgeführt...	0 %	DWM-1	84.6 MB
svchost.exe	1048	Wird ausgeführt...	0 %	SYSTEM	20.29 MB
svchost.exe	1068	Wird ausgeführt...	0 %	Lokaler Dienst	18.97 MB
svchost.exe	1124	Wird ausgeführt...	0 %	Netzwerkdienst	31.95 MB
avdlr.exe	1172	Wird ausgeführt...	0 %	N.D.C.	81.7 MB

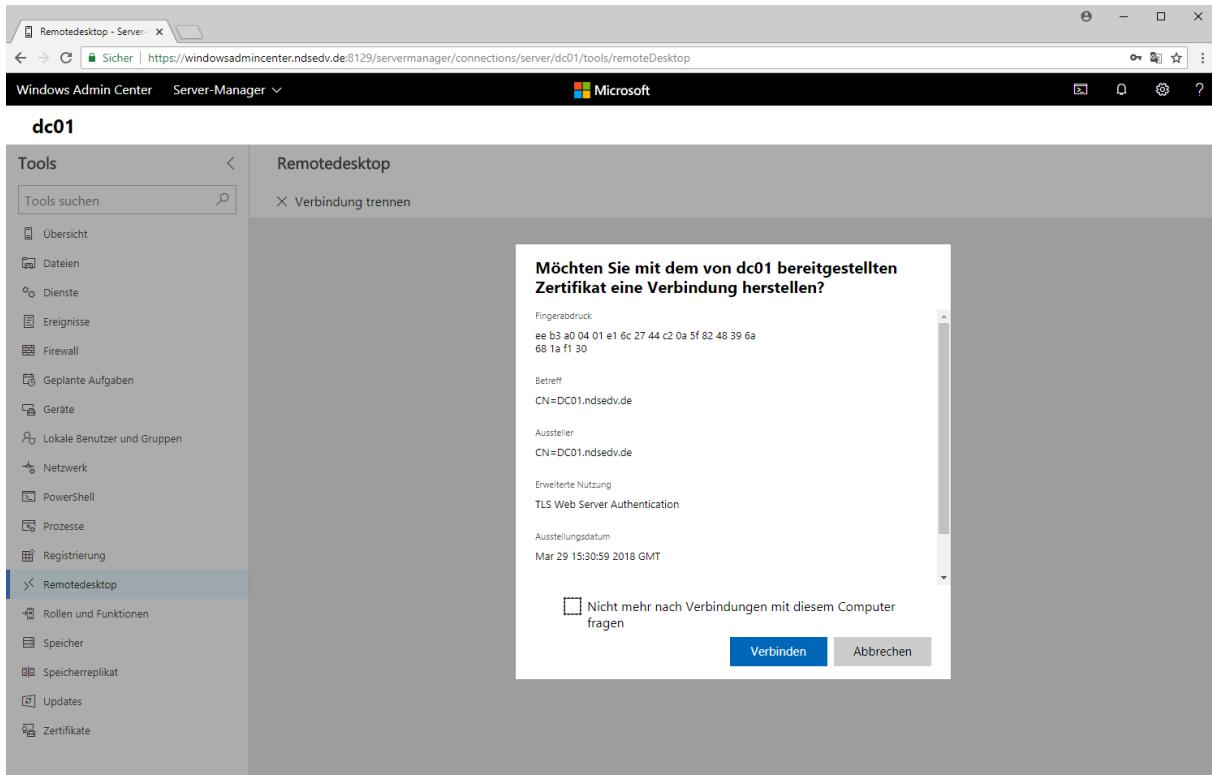
Registrierung:

The screenshot shows the Windows Admin Center interface for the server 'dc01'. The left sidebar is titled 'Tools' and lists various management options. The 'Registrierung' (Registry) tool is selected and active. The main pane shows the 'HKEY_LOCAL_MACHINE\SYSTEM' key. The left navigation pane shows a tree view of registry keys under 'Registrierung', including 'HKEY_CLASSES_ROOT', 'HKEY_CURRENT_USER', 'HKEY_LOCAL_MACHINE', 'HKEY_USERS', and 'HKEY_CURRENT_CONFIG'. The 'SYSTEM' key under 'HKEY_LOCAL_MACHINE' is currently selected. The right pane displays a table with columns for 'Name', 'Typ' (Type), and 'Daten' (Data). A message at the top right states '0 Elemente' (0 elements). Below the table, it says 'Keine Datensätze gefunden' (No data sets found).

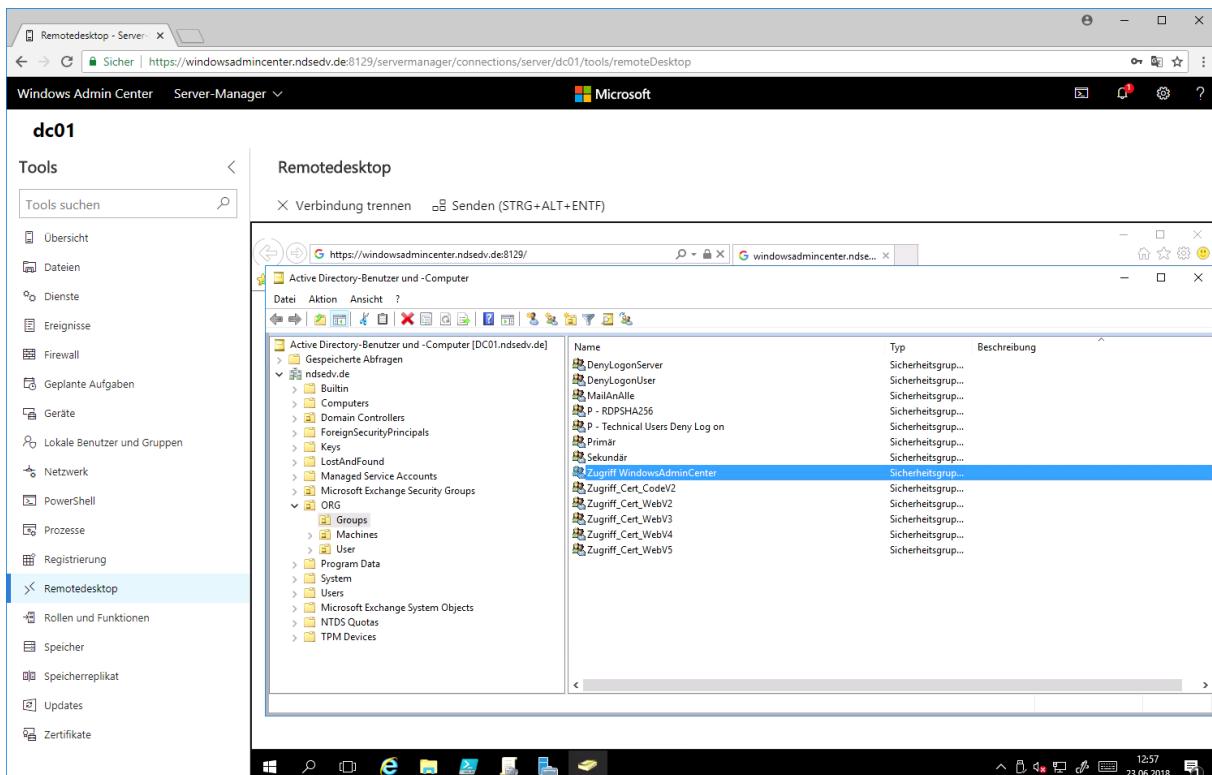


Windows Admin Center – Honolulu installieren

Remotedesktop:



Direktes Arbeiten auf der entfernten Station:





Windows Admin Center – Honolulu installieren

Rollen und Funktionen:

Name	Status	Typ
Rollen	5 von 95 installiert	
Active Directory-Lightweight Directory Services	Verfügbar	Role
Active Directory-Domänendienste	Installiert	Role
Active Directory-Rechteverwaltungsdienste	0 von 2 installiert	Role
Active Directory-Verbunddienste	Verfügbar	Role
Active Directory-Zertifikatdienste	0 von 6 installiert	Role
Datei-/Speicherdienste	2 von 12 installiert	Role
Device Health Attestation	Verfügbar	Role
DHCP-Server	Installiert	Role
DNS-Server	Installiert	Role
Druck- und Dokumentdienste	0 von 4 installiert	Role
Faxserver	Verfügbar	Role
Host Guardian-Dienst	Verfügbar	Role
Hyper-V	Verfügbar	Role
MultiPoint Services	Verfügbar	Role
Netzwerkcontroller	Verfügbar	Role
Netzwerkrichtlinien- und Zugriffsdienste	Verfügbar	Role
Remotedesktopdienste	0 von 6 installiert	Role
Remotezugriff	0 von 3 installiert	Role
Volumenaktivierungsdienste	Verfügbar	Role
Wählername (RS)	0 von 12 installiert	Role

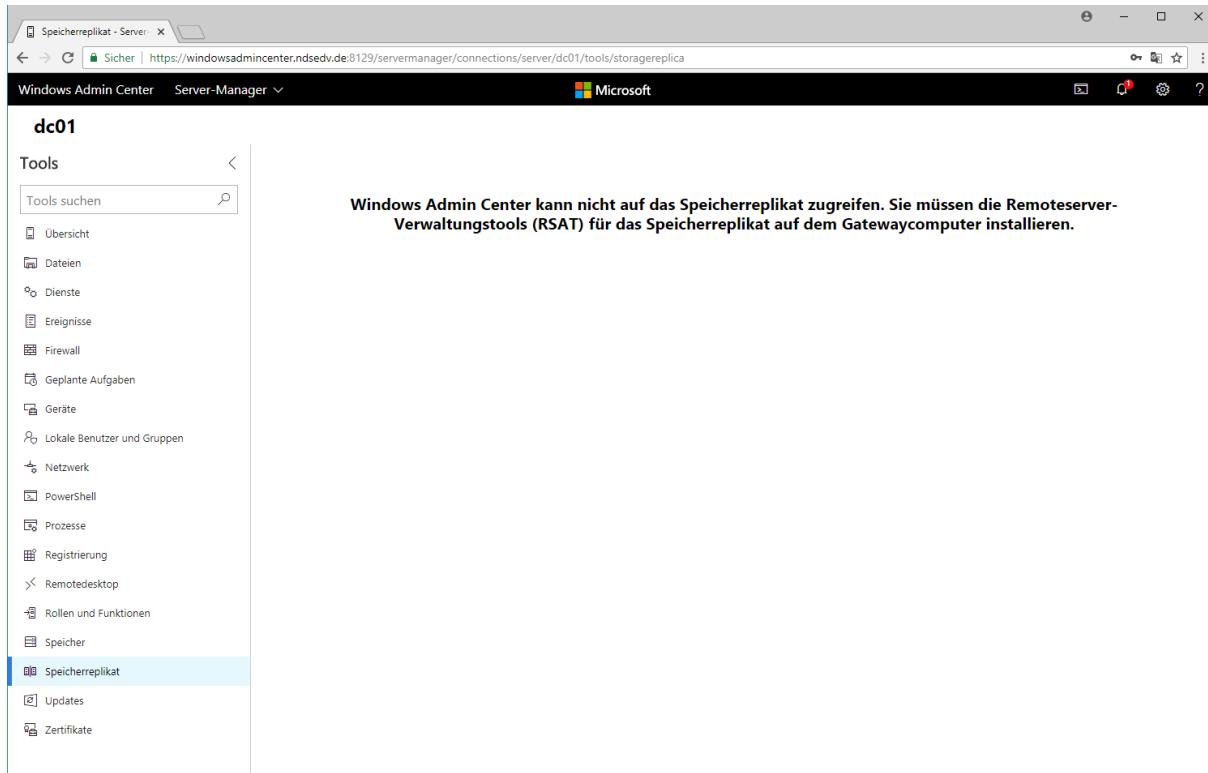
Speicher:

Name	Laufwerktyp	Zustand	Status	Dateisystem	Freier Speicherplatz	Große
(C)	Behoben	Fehlerfrei	OK	NTFS	37.1 GB	60 GB
VMware Tools (D)	CD-ROM	Fehlerfrei	OK	CDFS	0 B	98.6 MB



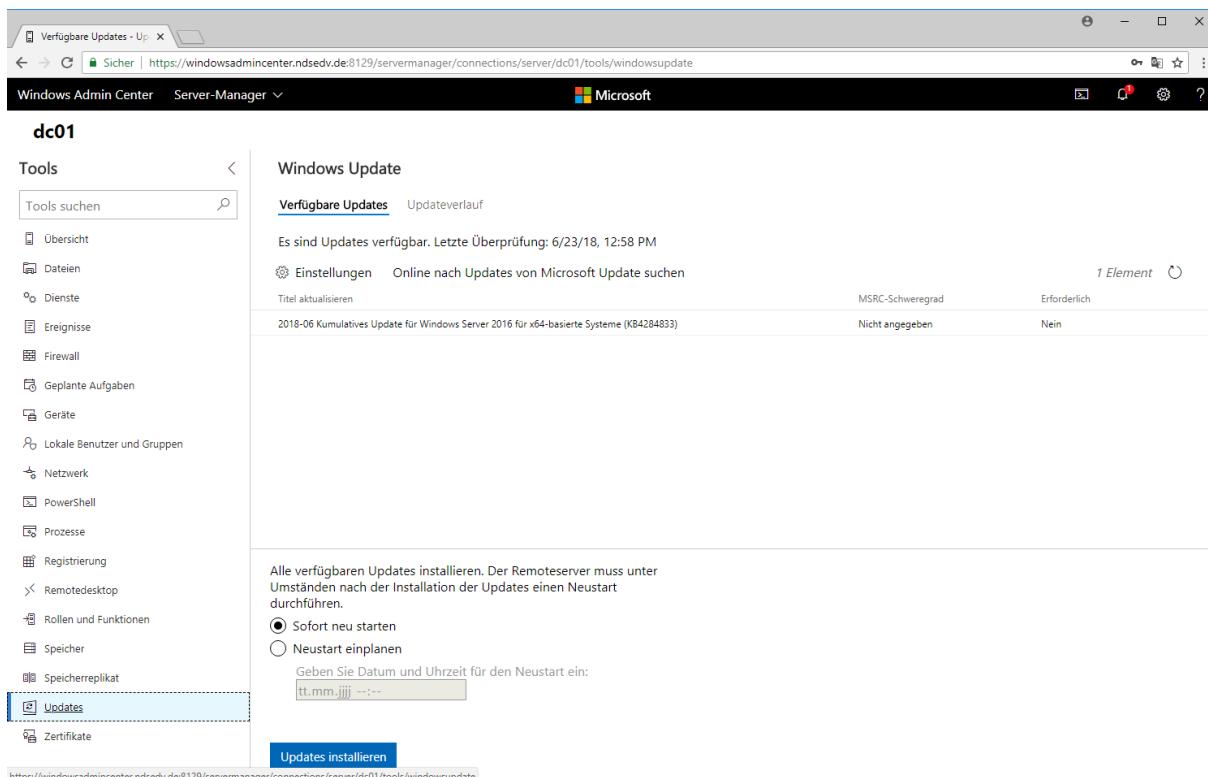
Windows Admin Center – Honolulu installieren

Speichergeräte:



Windows Admin Center kann nicht auf das Speicherreplikat zugreifen. Sie müssen die Remoteserver-Verwaltungstools (RSAT) für das Speicherreplikat auf dem Gatewaycomputer installieren.

Updates:



Windows Update

Verfügbare Updates Updateverlauf

Es sind Updates verfügbar. Letzte Überprüfung: 6/23/18, 12:58 PM

Einstellungen Online nach Updates von Microsoft Update suchen

Titel aktualisieren	MSRC-Schweregrad	Erforderlich
2018-06 Kumulatives Update für Windows Server 2016 für x64-basierte Systeme (KB4284833)	Nicht angegeben	Nein

Alle verfügbaren Updates installieren. Der Remoteserver muss unter Umständen nach der Installation der Updates einen Neustart durchführen.

Sofort neu starten
 Neustart einplanen

Geben Sie Datum und Uhrzeit für den Neustart ein:
[tt.mm.jjjj --:--]

Updates installieren



Windows Admin Center – Honolulu installieren

Zertifikate:

The screenshot shows the 'Certificates' tool in the Windows Admin Center. The left sidebar lists various tools like 'Übersicht', 'Dateien', 'Dienste', etc. The 'Zertifikate' tool is selected. The main area shows a table with four columns: 'ALLE' (132), 'ABGELAUFEN' (13), 'LÄUFT DEMNÄCHST AB' (1), and 'EREIGNISSE' (14). The 'ABGELAUFEN' column is highlighted.

Zertifikate verwalten!

The screenshot shows the 'Certificates' tool in the Windows Admin Center, specifically the 'Abgelaufen' (Expired) section. The left sidebar shows the 'Zertifikate' tool is selected. The main area displays a table of expired certificates with columns for 'Zertifikatsname', 'Status', 'Ausgestellt am', 'Ablaufdatum', 'Fingerabdruck', 'Zertifikatspeicher', and 'Logischer S...'. The table lists various certificates from Microsoft and other issuers, such as 'Microsoft Authen...', 'Copyright (c) 199...', 'NO LIABILITY AC...', 'Microsoft IT SSL S...', 'www.verisign.com...', 'Microsoft Windo...', 'NDS', 'Microsoft Authen...', 'Copyright (c) 199...', 'NO LIABILITY AC...', 'www.verisign.com...', 'Microsoft Windo...', and 'DC01.ndsedv.de'. The 'Details' section at the bottom is expanded.



Windows Admin Center – Honolulu installieren

Details von Zertifikaten anzeigen lassen!

Zertifikate

Zertifikatspeicher Ereignisse

↓ Exportieren ⌂ Erneuern Mehr ↴ 13 Elemente ⌂ Suchen

Zertifikatsname	Status	Ausgestellt am	Ablaufdatum	Fingerabdruck	Zertifikatspeicher	Logischer S...
Copyright (c) 199...	Abgelaufen	13.5.1997	31.12.1999	245C97DF7514E7...	Root	LocalMachine...
NO LIABILITY AC...	Abgelaufen	12.5.1997	8.1.2004	18F7C1FCC30902...	Root	LocalMachine...
www.verisign.co...	Abgelaufen	17.4.1997	25.10.2016	D559A586669B00...	CA	LocalMachine...
Microsoft Windo...	Abgelaufen	1.10.1997	31.12.2002	109F1CAED645B...	CA	LocalMachine...
DC01.ndsedv.de	Abgelaufen	19.11.2016	19.11.2017	DFCE44CA7D098...	My	LocalMachine...

Details - DC01.ndsedv.de

Archiviert: NotArchived Zertifikatsname: DC01.ndsedv.de

Erweiterte Schlüsselverwendung: Anzeigename: DC01.ndsedv.de

Serverauthentifizierung 1.3.6.1.5.5.7.3.1 Clientauthentifizierung 1.3.6.1.5.5.7.3.2

Ausstellername: ISSUINGCA Ausgestellt für: DC01.ndsedv.de

Pfad: LocalMachine\My\DFCE44CA7D09853A618B86E 19.11.2016 07935327PE7692673

Gültig bis: 19.11.2017 Privater Schlüssel: Nicht exportierbar

Öffentlicher Schlüssel: RSA Parameter des öffentlichen Schlüssels: 05 00

Ab sofort steht uns der Dienst (Gateway Server) netzwerkweit zur Verfügung:

Rufe den Dienst (WAC) nun vom DC01 auf, um den Server SRV00 zu administrieren.

Übersicht

Neu starten Herunterfahren Datenträgermetriken aktivieren Computer-ID bearbeiten Mehr ↴

Computername:	Domäne:	Betriebssystem:
srv00	ndsedv.de	Microsoft Windows Server 2016 Standard
Version:	Installierter Speicher (RAM):	Speicherplatz gesamt:
10.0.14393	2 GB	60 GB
Prozessoren:	Hersteller:	Modell:
Intel(R) Core(TM) i7-5820K CPU @ 3.30GHz	VMware, Inc.	VMware Virtual Platform
Logische Prozessoren:	Freier Speicherplatz:	NIC(s)
2	36.18 GB	1
Betriebszeit:	Anzahl der Benutzer:	
0:05:54	1	

CPU

Auslastung: 1.45% Handles: 22546
Geschwindigkeit: 3.37GHz
Prozesse: 52
Threads: 949



Windows Admin Center – Honolulu installieren

Rufe den Dienst (WAC) nun vom DC01 auf, um den Server IssuingCA zu administrieren.

The screenshot shows the Windows Admin Center interface for the server **issuingca.ndsedv.de**. The left sidebar is the 'Tools' navigation menu. The 'Zertifikate' (Certificates) tool is selected and highlighted in blue. The main content area is titled 'Zertifikate' and shows a list of certificates under 'Zertifikatspeicher' (Certificate Store). The 'CA' (Certificate Authority) node is selected. The table lists several certificates, including 'ISSUINGCA' (selected), 'Root Agency', 'AuthRoot', 'ClientAuthIssuer', 'Disallow', 'FlightRoot', 'KRA', 'MSIEHistoryJournal', 'My', 'Remote Desktop', 'REQUEST', 'Root', 'SmartCardRoot', 'Trust', 'TrustedDevices', 'TrustedPeople', 'TrustedPublisher', 'WebHosting', and 'Windows Live ID Token Issuer'. The 'Details - ISSUINGCA' pane on the right provides specific details for the selected certificate, including its name, issuer, validity period, and key usage.

Lokale Benutzer und Gruppen verwalten:

The screenshot shows the Windows Admin Center interface for the server **issuingca.ndsedv.de**. The left sidebar is the 'Tools' navigation menu. The 'Lokale Benutzer und Gruppen' (Local Users and Groups) tool is selected and highlighted in blue. The main content area is titled 'Lokale Benutzer und Gruppen' and shows a list of users under the 'Benutzer (4)' tab. The table lists four users: 'admin', 'Administrator', 'DefaultAccount', and 'Gast'. The 'Gruppen (24)' tab is also visible. The 'Details' pane on the right shows the properties for the 'Administrator' user, including its full name, description, and a note that it is a pre-defined account for managing the computer.



Windows Admin Center – Honolulu installieren

Füge nun einen Windows 10 Client zur Verwaltung hinzu:

The screenshot shows the Windows Admin Center interface for managing computer connections. A modal dialog box is open, titled 'Computer hinzufügen'. It contains fields for 'Name' (set to 'Win10Ent') and 'Passwort' (set to '*****'). Below these are 'Anmelden' (Login) and 'Abbrechen' (Cancel) buttons. To the right of the dialog, a message says 'Geben Sie den Namen des zu verwaltenden Computers ein:' (Enter the name of the computer to be managed). A text input field also contains 'Win10Ent'. At the bottom right of the dialog are 'Übermitteln' (Send) and 'Abbrechen' (Cancel) buttons.

Auf dieser Weise lassen sich die wichtigsten Aufgaben aus der Ferne erledigen:

The screenshot shows the 'Übersicht' (Overview) page for the computer 'win10ent.ndsedv.de'. The left sidebar shows a list of tools: Übersicht, Dienste, Ereignisse, Firewall, Geplante Aufgaben, Geräte, Lokale Benutzer und Gruppen, PowerShell, Prozesse, Registrierung, Remotedesktop, Speicher, and Zertifikate. 'Übersicht' is currently selected. The main area displays general information about the computer, including its name ('win10ent'), domain ('ndsedv.de'), operating system ('Microsoft Windows 10 Enterprise'), version ('10.0.16299'), RAM ('2 GB'), and processor ('Intel(R) Core(TM) i7-5820K CPU @ 3.30GHz'). It also shows logical processors ('Freier Speicherplatz'), memory ('NIC(s)'), and CPU usage graphs. The CPU graph shows a sharp peak in usage, with metrics like 'Auslastung 2%', 'Geschwindigkeit 3.37GHz', 'Prozesse 71', and 'Threads 1252'. The Speicher (Memory) graph shows 'Auslastung 65.2%' and 'Zugesichert 1.4GB'.



Windows Admin Center – Honolulu installieren

Einen Failover Cluster fügt man auf dieselbe Weise hinzu:

The screenshot shows the Windows Admin Center interface with the 'Failovercluster-Manager' tab selected. On the left, there is a list of 'Failoverclusterverbindungen' with options to 'Hinzufügen', 'Verbinden', 'Verwalten als', 'Entfernen', and 'Tags bearbeiten'. A note at the bottom says: 'Fügen Sie zunächst mit dem Befehl „+ Hinzufügen“ eine Verbindung zu „Windows Admin Center“ hinzu.' On the right, a 'Verbindung „Failovercluster“ hinzufügen' dialog is open. It has tabs for 'Verbindungstags' and 'Cluster hinzufügen' (which is selected). Below these are fields for 'Clustername' (with placeholder 'Clusternamen eingeben') and 'Tags hinzufügen'. At the bottom are 'Übermitteln' and 'Abbrechen' buttons.

Core Server administrieren:

Auf Windows Core Servern ist winrm –quickconfig zu konfigurieren um die Server mit WAC verwalten zu können.

The screenshot shows a Windows Command Prompt window with the command 'C:\Windows\System32\cmd.exe'. The output of the 'winrm –quickconfig' command is displayed, showing various configuration options. The 'Remoteverwaltung konfigurieren' option is listed with the value 'Aktiviert' (Enabled), and a red arrow points to this line. Other options listed include Domäne/Arbeitsgruppe, Computername, Lokalen Administrator hinzufügen, Windows Update-Einstellungen, Updates herunterladen u. installieren, Remotedesktop, Netzwerkeinstellungen, Datum und Uhrzeit, Telemetrieinstellungen, Windows-Aktivierung, Benutzer abmelden, Server neu starten, Server herunterfahren, and Zur Befehlszeile wechseln. The prompt at the bottom says 'Geben Sie eine Zahl ein, um eine Option auszuwählen:'.



Windows Admin Center – Honolulu installieren

Windows Admin Center - Gatewayzugriff konfigurieren:

Gatewayadministratoren dürfen sich an das WAC anmelden und haben zusätzlich das Recht die Zugriffe zu administrieren. Ein Gatewaybenutzer darf sich nur an das WAC anmelden. Eine Verwaltung der hinterlegten Server erfordert weitere Berechtigungen.

Einstellungen

Allgemein

Gatewayzugriff

Identitätsanbieter

Active Directory oder lokale Gruppen

Azure

Ändern

Steuerung des Zugriffs auf das Gateway

Fügen Sie Gruppen hinzu, um zu steuern, wer Zugriff auf das Gateway hat. Für die mehrstufige Authentifizierung müssen sich Gatewaybenutzer in einer der zulässigen Gruppen befinden und sich bei einer sekundären Gruppe authentifizieren, z. B. einer Gruppe, die Smartcard-Authentifizierung bietet.

Gatewaybenutzer Gatewayadministratoren

+ Hinzufügen - Löschen

Name	Typ
VORDEFINIERT\Administatoren	SecurityGroup
Zugriff WindowsAdminCenter	SecurityGroup

2 Elemente 1 ausgewählt X Suchen

Schließen

Rollenbasierte Zugriffssteuerung für die zu administrierenden Server einrichten:

Übersicht

Neu starten Herunterfahren Datenträgermetriken aktivieren Computer-ID bearbeiten Einstellungen Aktualisieren

Computername: srv00 Domäne: ndsedv.de Betriebssystem: Microsoft Windows Server 2016 Standard

Version: 10.0.14393 Installierter Speicher (RAM): 2 GB Speicherplatz gesamt: 60 GB

Prozessoren: Intel(R) Core(TM) i7-5820K CPU @ 3.30GHz Hersteller: VMware, Inc. Modell: VMware Virtual Platform

Logische Prozessoren: 2 Freier Speicherplatz: 44.59 GB NIC(s): 1

CPU

Auslastung: 6.39% Handles: 31395

Geschwindigkeit: 3.37GHz Betriebszeit: 0:1:4:40

Prozesse: 72 Threads: 1041

Vor 60 Sekunden Jetzt

Sneicher

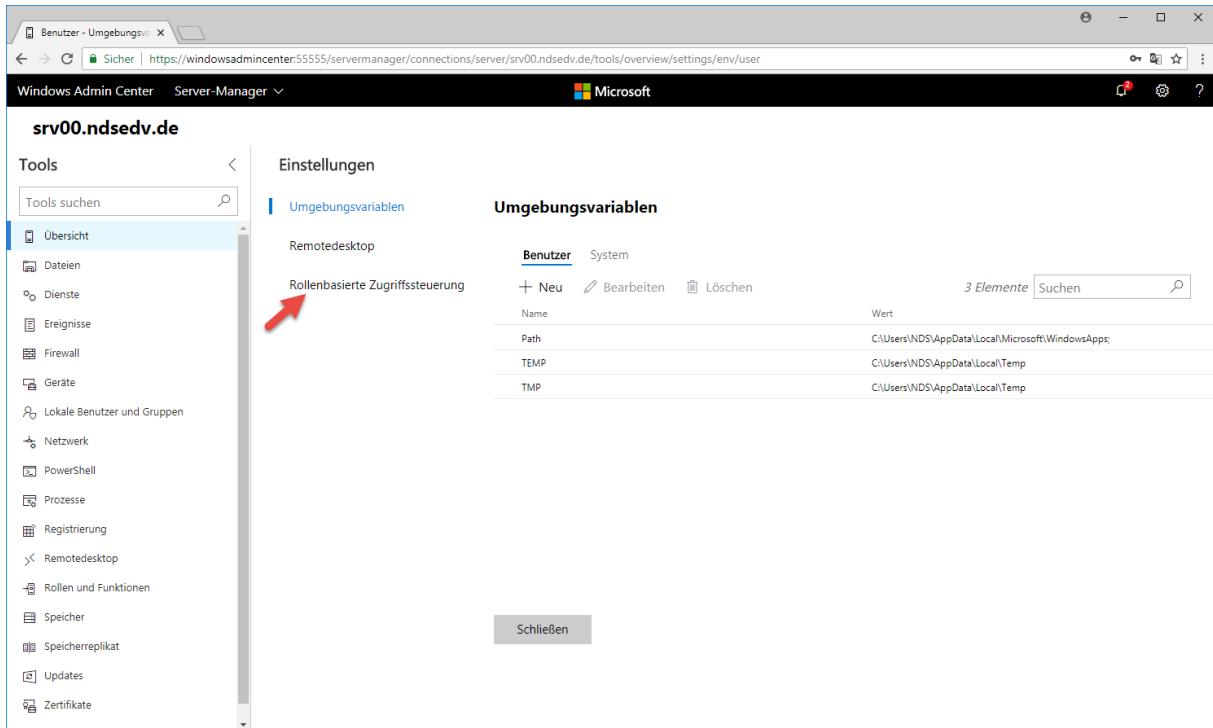
Auslastung: 100% Zugesichert

https://windowsadmincenter:55555/servermanager/connections/server/srv00.ndsedv.de/tools/overview



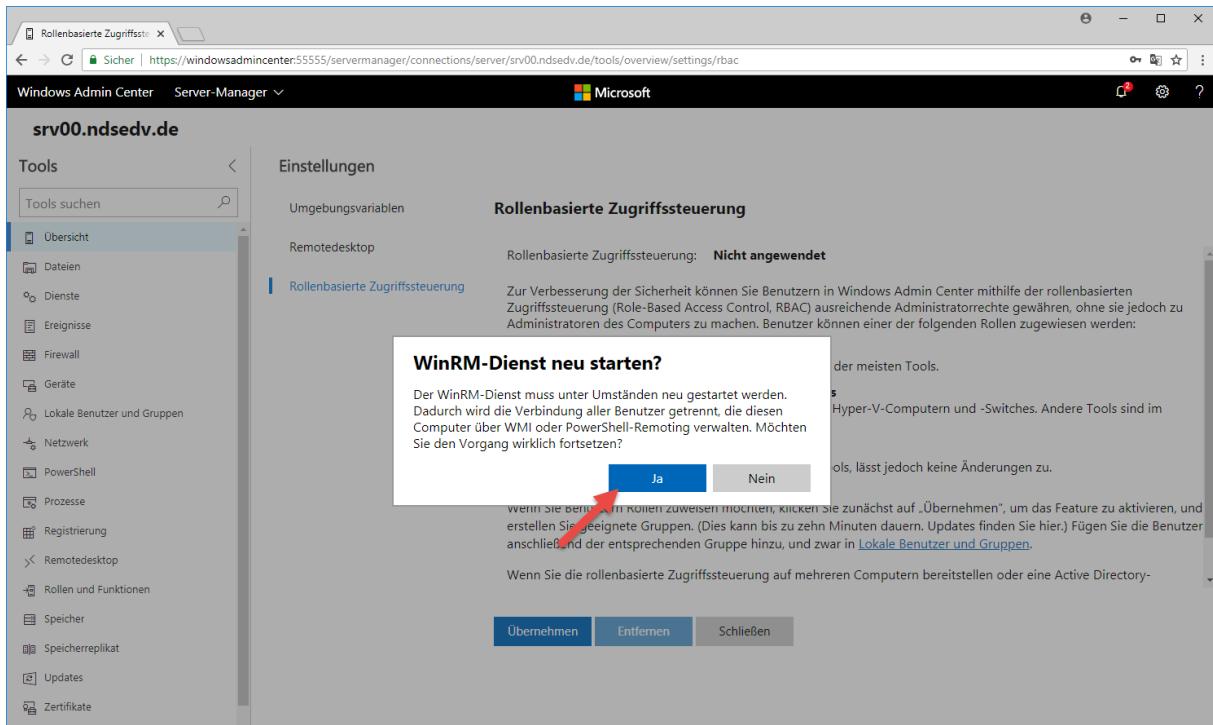
Windows Admin Center – Honolulu installieren

Rollenbasierte Zugriffssteuerung auswählen



The screenshot shows the Windows Admin Center interface for the server 'srv00.ndsedv.de'. The left sidebar is titled 'Tools' and lists various management options. The main content area is titled 'Einstellungen' (Settings) and shows the 'Umgebungsvariablen' (Environment Variables) section under 'Rollenbasierte Zugriffssteuerung' (Role-Based Access Control). The 'Benutzer' tab is selected, showing a list of environment variables with their names and paths. A red arrow points to the 'Rollenbasierte Zugriffssteuerung' link in the sidebar.

WinRM neu starten. Auf dem Zielsystem werden nun neue Sicherheitsgruppen angelegt.

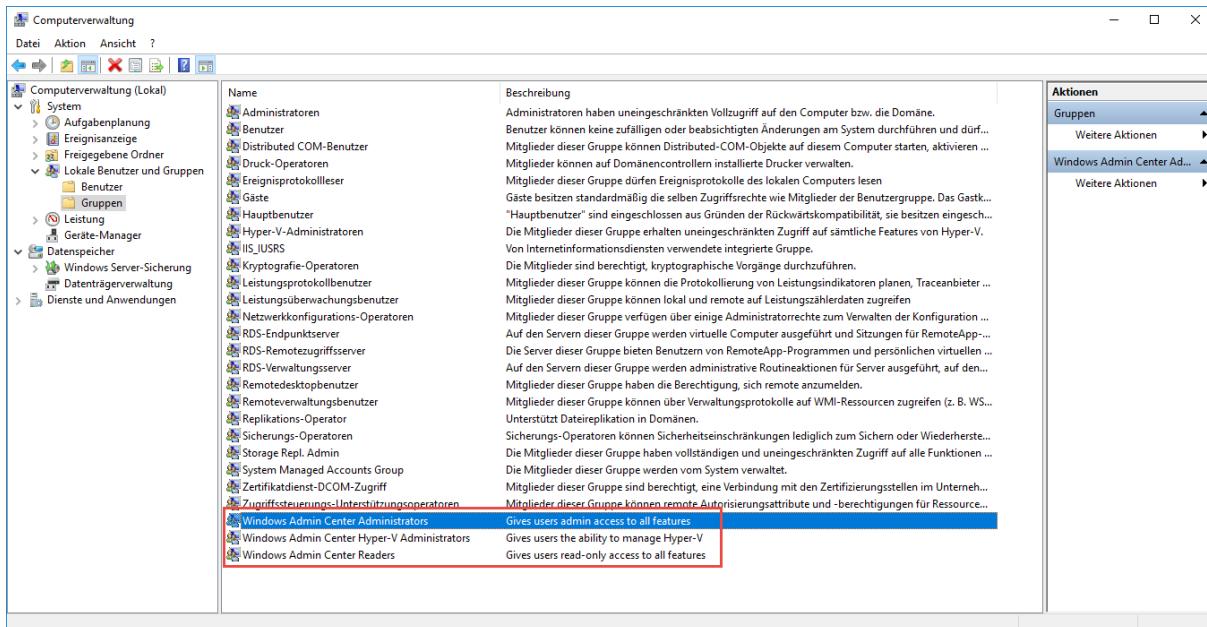


The screenshot shows the Windows Admin Center interface for the server 'srv00.ndsedv.de'. The left sidebar is titled 'Tools' and lists various management options. The main content area is titled 'Einstellungen' (Settings) and shows the 'Rollenbasierte Zugriffssteuerung' (Role-Based Access Control) section. A modal dialog box titled 'WinRM-Dienst neu starten?' (WinRM service restart?) is displayed. The dialog contains text explaining that the WinRM service must be restarted to apply RBAC changes. It includes a 'Ja' (Yes) button highlighted with a red arrow and a 'Nein' (No) button.



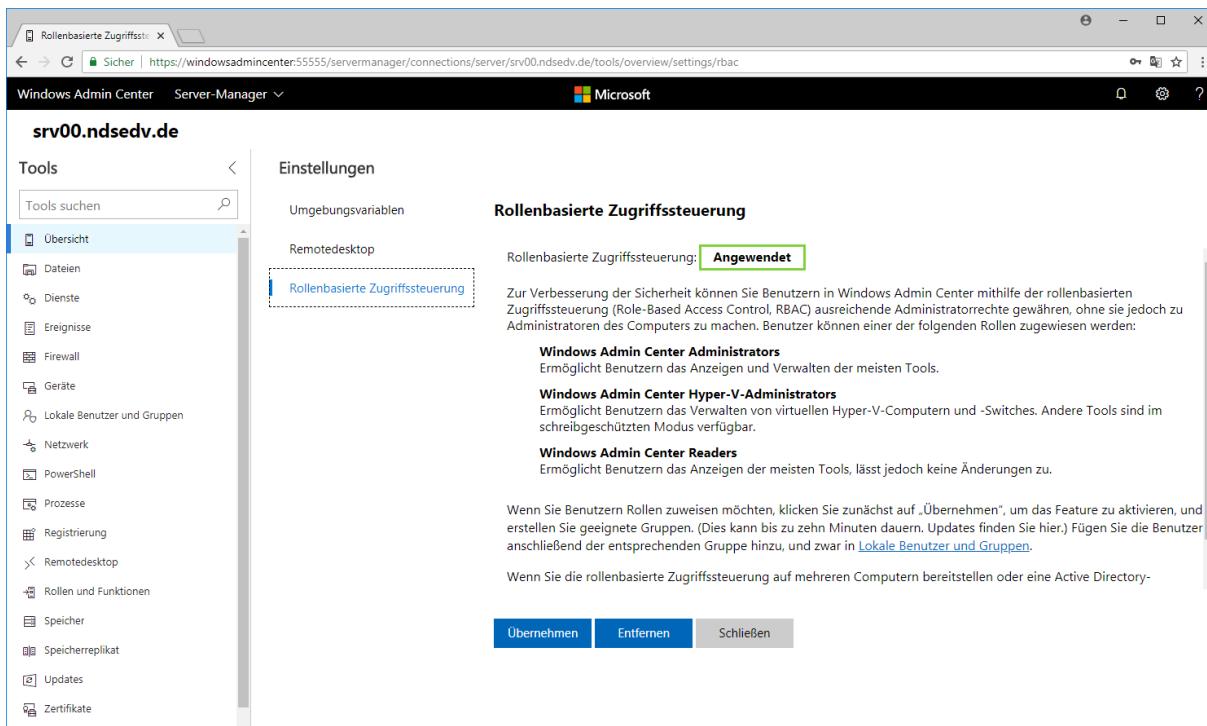
Windows Admin Center – Honolulu installieren

Das sind die neuen Sicherheitsgruppen die zur granularen Verwaltung eingesetzt werden können.



The screenshot shows the Windows Admin Center interface for local computer management. The 'Gruppen' (Groups) section is highlighted with a red box. The group 'Windows Admin Center Administrators' is described as giving users admin access to all features. Other groups listed include Administratoren, Benutzer, Distributed COM-Benutzer, Druck-Operatoren, Ereignisprotokolleser, Gäste, Hauptbenutzer, Hyper-V-Administratoren, IIS_JURS, Kryptografie-Operatoren, Leistungsprotokollbenutzer, Leistungsüberwachungsbenutzer, Netzwerkonfigurations-Operatoren, RDS-Endpunktserver, RDS-Remotezugriffsserver, RDS-Verwaltungsserver, Remotedesktopbenutzer, Remoteverwaltungsbenutzer, Replikations-Operator, Sicherungs-Operatoren, Storage Repl. Admin, System Managed Accounts Group, Zertifikatdienst-DCOM-Zugriff, Zugriffssteuerungs-Unterstützungsoptoren, Windows Admin Center Hyper-V Administrators, and Windows Admin Center Readers.

Über das WAC bekommen wir nun die Rückmeldung das die rollenbasierte Zugriffssteuerung aktiviert wurde.

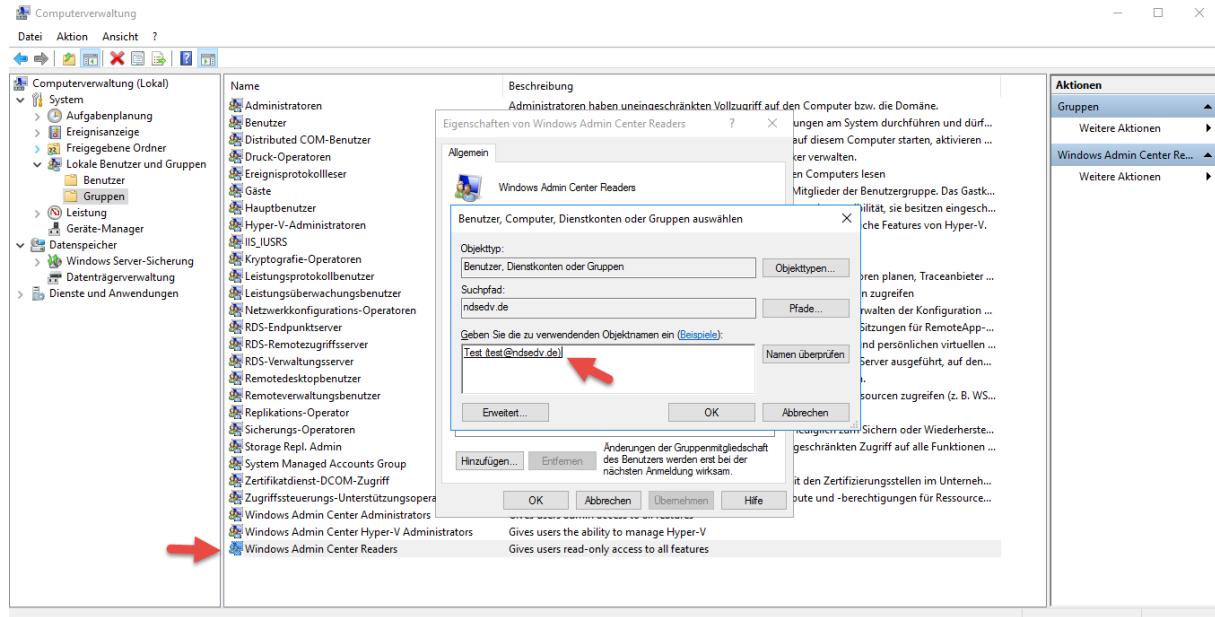


The screenshot shows the Windows Admin Center interface for role-based access control settings. The 'Rollenbasierte Zugriffssteuerung' (Role-Based Access Control) section is highlighted with a red box. It shows that the feature is applied ('Angewendet'). The 'Windows Admin Center Administrators' role is listed as giving users admin access to all features. Other roles listed include 'Windows Admin Center Hyper-V Administrators' and 'Windows Admin Center Readers'. The interface also includes sections for 'Umgebungsvariablen' (Environment Variables) and 'Remotedesktop' (Remotedesktop). Buttons at the bottom include 'Übernehmen' (Accept), 'Entfernen' (Remove), and 'Schließen' (Close).

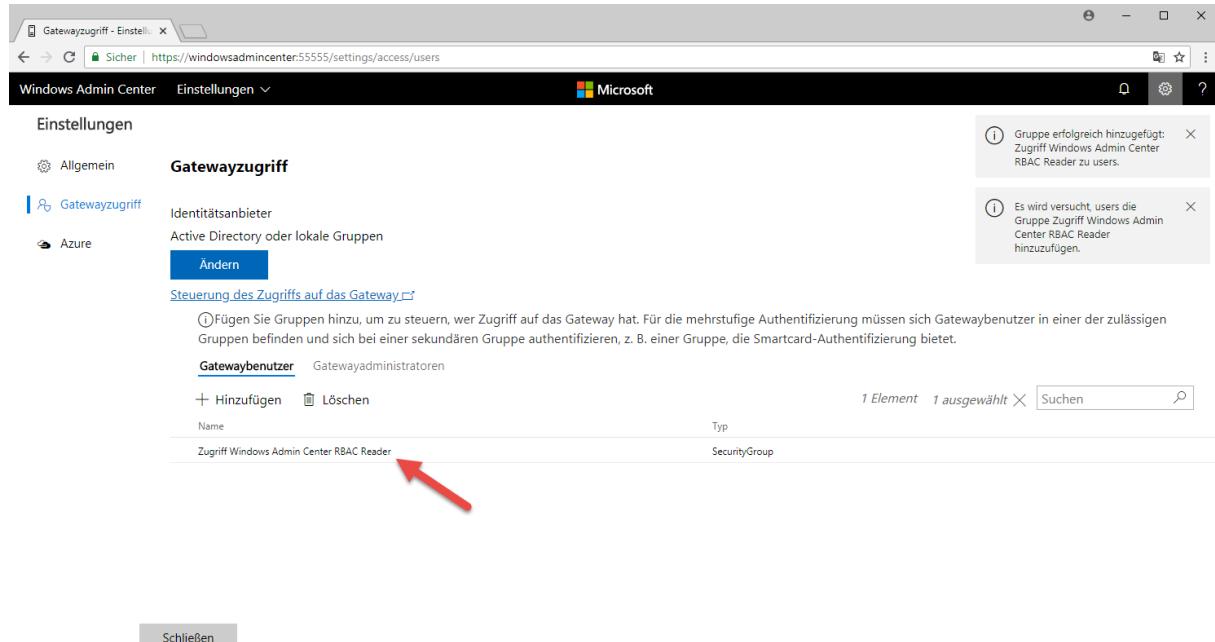


Windows Admin Center – Honolulu installieren

Der User Test wird nun Mitglied der Gruppe WAC Readers



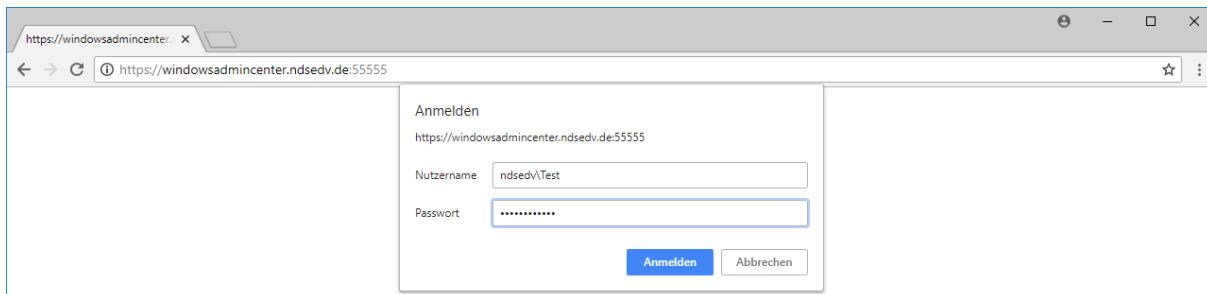
Im Windows Admin Center ist der User Test Mitglied der Gruppe „Zugriff Windows Admin Center RBAC Reader“.





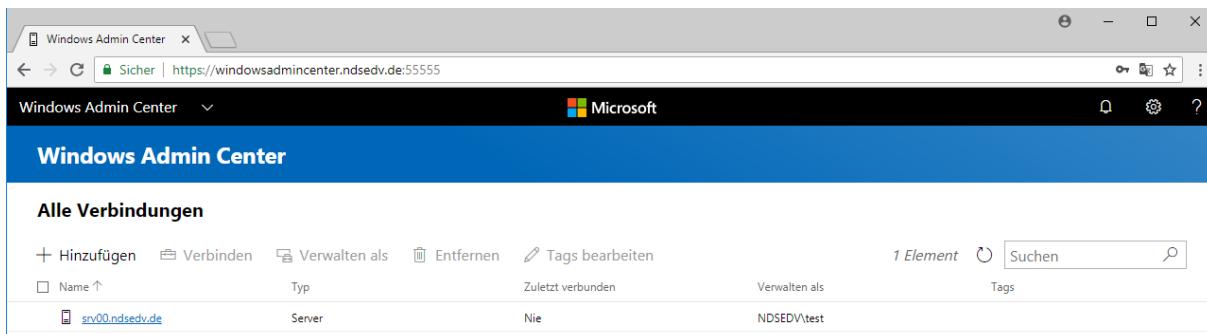
Windows Admin Center – Honolulu installieren

Anmeldung an das WAC:



Anmelden
https://windowsadmincenter.ndsedv.de:55555
Username: ndsedv\test
Passwort: *****
Anmelden Abbrechen

Der User Test konnte sich erfolgreich an das WAC anmelden.

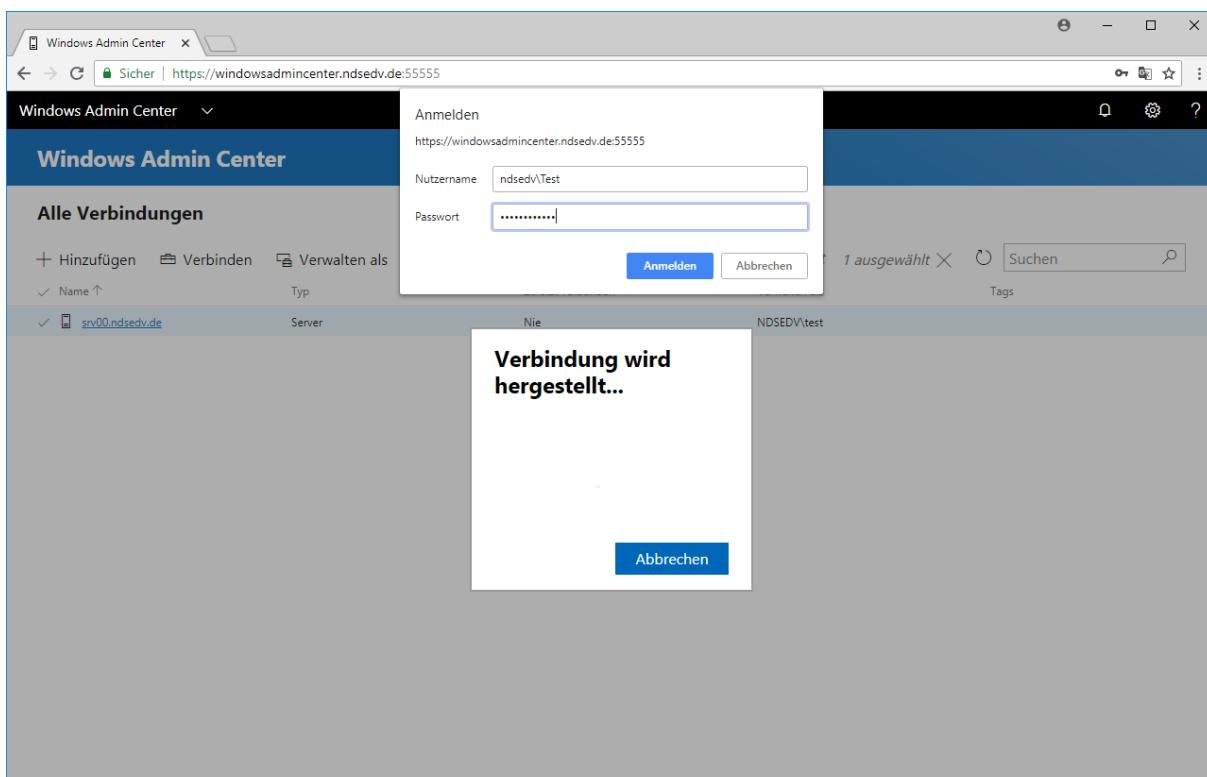


Windows Admin Center

Alle Verbindungen

Alle Verbindungen			
Name		Type	Zuletzt verbunden
<input type="checkbox"/> srv00.ndsedv.de		Server	Nie

1 Element Suchen



Windows Admin Center

Alle Verbindungen

Anmelden
https://windowsadmincenter.ndsedv.de:55555
Username: ndsedv\test
Passwort: *****
Anmelden Abbrechen

1 ausgewählt Suchen

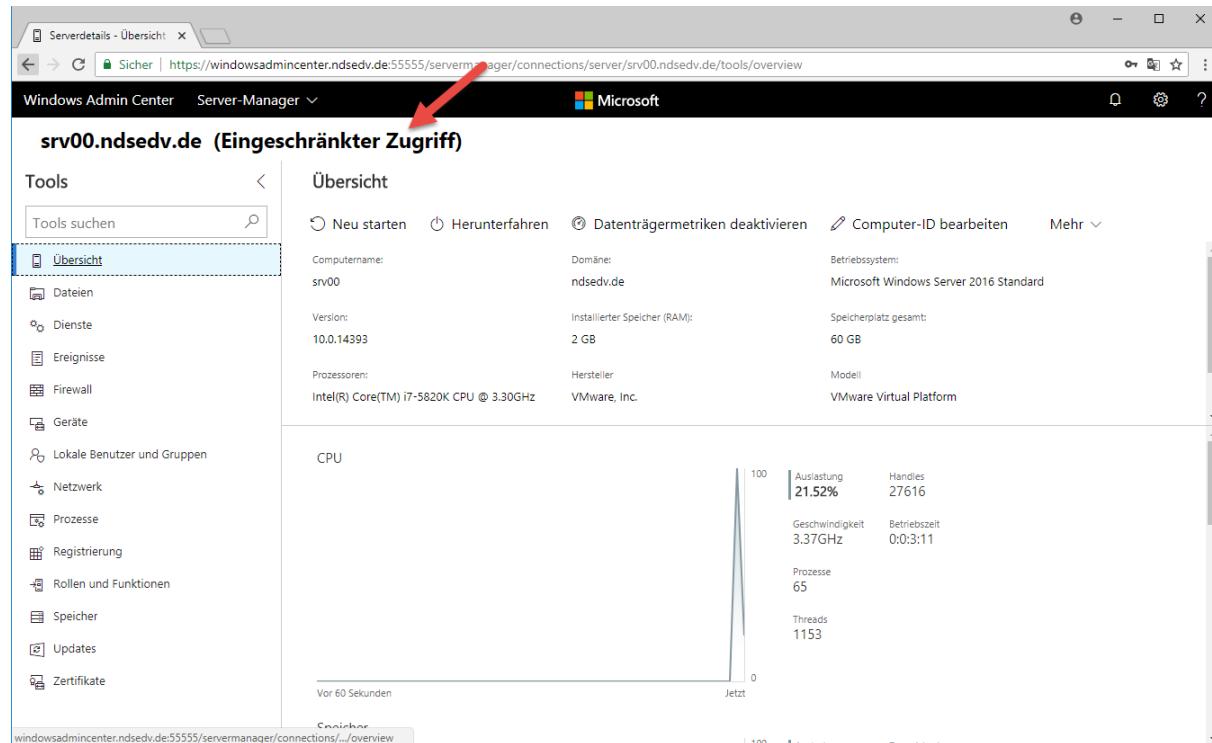
Verbindung wird hergestellt...

Abbrechen



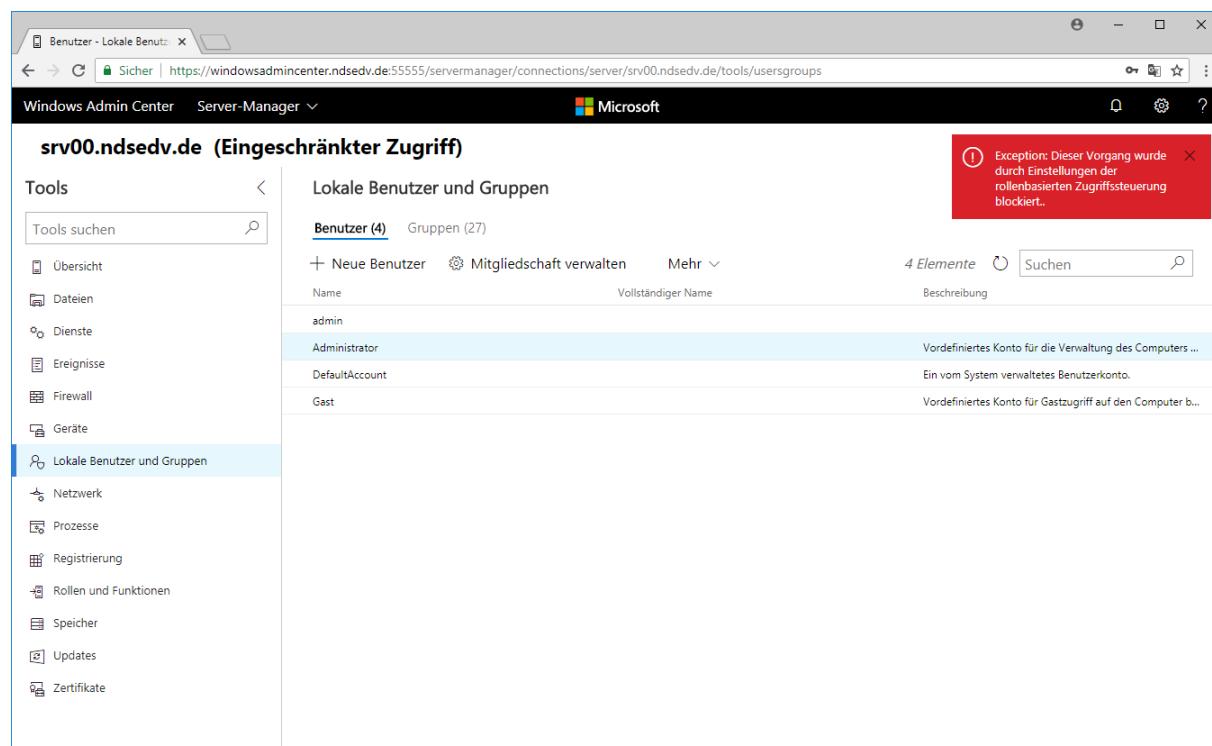
Windows Admin Center – Honolulu installieren

Der Benutzer Test hat nun eingeschränkte Rechte; nur Daten und Informationen zu lesen aber nicht zu verändern.



The screenshot shows the Windows Admin Center interface for the server 'srv00.ndsedv.de'. A red arrow points to the title bar which displays '(Eingeschränkter Zugriff)' (restricted access). The main content area shows an 'Übersicht' (Overview) of the server's hardware and performance. The left sidebar has 'Lokale Benutzer und Gruppen' (Local Users and Groups) selected.

Wenn versucht wird, eine Aktion auszuführen für die man nicht berechtigt ist, erscheint eine Fehlermeldung oder Warnhinweis.



The screenshot shows the Windows Admin Center interface for the server 'srv00.ndsedv.de'. The title bar shows '(Eingeschränkter Zugriff)'. The main content area shows the 'Lokale Benutzer und Gruppen' (Local Users and Groups) page. A red box highlights an error message: 'Exception: Dieser Vorgang wurde durch Einstellungen der rollenbasierten Zugriffssteuerung blockiert.' (Exception: This action was blocked by the settings of the role-based access control). The left sidebar has 'Lokale Benutzer und Gruppen' selected.



Windows Admin Center – Honolulu installieren

Troubleshooting & Tipps:

Hergestellte Verbindungen vom SRV00 > DC01

```
Administrator: Eingabeaufforderung
C:\Windows\system32>netstat -ano | find "5985"
TCP  0.0.0.0:5985      0.0.0.0:0          ABHÖREN      4
TCP  172.18.32.110:51647 172.18.32.31:5985  WARTEND      0
TCP  172.18.32.110:51648 172.18.32.31:5985  WARTEND      0
TCP  172.18.32.110:51676 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:51677 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:51678 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:51687 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:51688 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:51690 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:51691 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:51694 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:51901 172.18.32.31:5985  WARTEND      0
TCP  172.18.32.110:51902 172.18.32.31:5985  WARTEND      0
TCP  172.18.32.110:51903 172.18.32.31:5985  WARTEND      0
TCP  172.18.32.110:51904 172.18.32.31:5985  WARTEND      0
TCP  172.18.32.110:52032 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:52033 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:52034 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:52035 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:52125 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:52126 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:52127 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:52128 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:52251 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:52252 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:52253 172.18.32.31:5985  HERGESTELLT  1916
TCP  172.18.32.110:52254 172.18.32.31:5985  HERGESTELLT  1916
TCP  [::]:5985          [::]:0          ABHÖREN      4

C:\Windows\system32>hostname
SRV00

C:\Windows\system32>
```

```
Administrator: Eingabeaufforderung
C:\Windows\system32>netstat -ano | find "5985"
TCP  0.0.0.0:5985      0.0.0.0:0          ABHÖREN      4
TCP  172.18.32.31:5985 172.18.32.110:51635  WARTEND      0
TCP  172.18.32.31:5985 172.18.32.110:51636  WARTEND      0
TCP  172.18.32.31:5985 172.18.32.110:51647  HERGESTELLT  4
TCP  172.18.32.31:5985 172.18.32.110:51648  HERGESTELLT  4
TCP  172.18.32.31:5985 172.18.32.110:51676  HERGESTELLT  4
TCP  172.18.32.31:5985 172.18.32.110:51677  HERGESTELLT  4
TCP  172.18.32.31:5985 172.18.32.110:51678  HERGESTELLT  4
TCP  172.18.32.31:5985 172.18.32.110:51687  HERGESTELLT  4
TCP  172.18.32.31:5985 172.18.32.110:51688  HERGESTELLT  4
TCP  172.18.32.31:5985 172.18.32.110:51690  HERGESTELLT  4
TCP  172.18.32.31:5985 172.18.32.110:51691  HERGESTELLT  4
TCP  172.18.32.31:5985 172.18.32.110:51694  HERGESTELLT  4
TCP  [::]:5985          [::]:0          ABHÖREN      4
UDP  0.0.0.0:55985     *:*           2496

C:\Windows\system32>hostname
DC01

C:\Windows\system32>netstat -ano | find "443"
TCP  172.18.32.31:50254  13.92.211.120:443  HERGESTELLT  3736
TCP  172.18.32.31:50260  13.92.211.120:443  HERGESTELLT  1512
UDP  0.0.0.0:56443       *:*           2496
UDP  0.0.0.0:57443       *:*           2496

C:\Windows\system32>
```



Windows Admin Center – Honolulu installieren

WINRM Konfiguration auf SRV00 auslesen:

winrm get winrm/config

```
Administrator: Windows PowerShell
PS C:\Windows\system32> winrm get winrm/config
Config
  MaxEnvelopeSizekb = 500
  MaxTimeoutms = 60000
  MaxBatchItems = 32000
  MaxProviderRequests = 4294967295
  Client
    NetworkDelayms = 5000
    URLPrefix = wsman
    AllowUnencrypted = false
    Auth
      Basic = true
      Digest = true
      Kerberos = true
      Negotiate = true
      Certificate = true
      CredSSP = false
    DefaultPorts
      HTTP = 5985
      HTTPS = 5986
    TrustedHosts = *
  Service
    RootSDL = O:NGS:BAD:P(A;;GA;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;WD)(AU;SA;GXGW;;WD)
    MaxConcurrentOperations = 4294967295
    MaxConcurrentOperationsPerUser = 1500
    EnumerationTimeoutms = 240000
    MaxConnections = 300
    MaxPacketRetrievalTimeSeconds = 120
    AllowUnencrypted = false [Source="GPO"]
    Auth
      Basic = true [Source="GPO"]
      Kerberos = true [Source="GPO"]
      Negotiate = true [Source="GPO"]
      Certificate = false
      CredSSP = false [Source="GPO"]
      CbtHardeningLevel = Relaxed
    DefaultPorts
      HTTP = 5985
      HTTPS = 5986
    IPv4Filter = * [Source="GPO"]
    IPv6Filter = * [Source="GPO"]
    EnableCompatibilityHttpListener = false [Source="GPO"]
    EnableCompatibilityHttpsListener = true [Source="GPO"]
    CertificateThumbprint
    AllowRemoteAccess = true [Source="GPO"]
  Winrs
    AllowRemoteShellAccess = true
    IdleTimeout = 7200000
    MaxConcurrentUsers = 2147483647
    MaxShellRunTime = 2147483647
    MaxProcessesPerShell = 2147483647
    MaxMemoryPerShellMB = 2147483647
    MaxShellsPerUser = 2147483647
PS C:\Windows\system32>
```

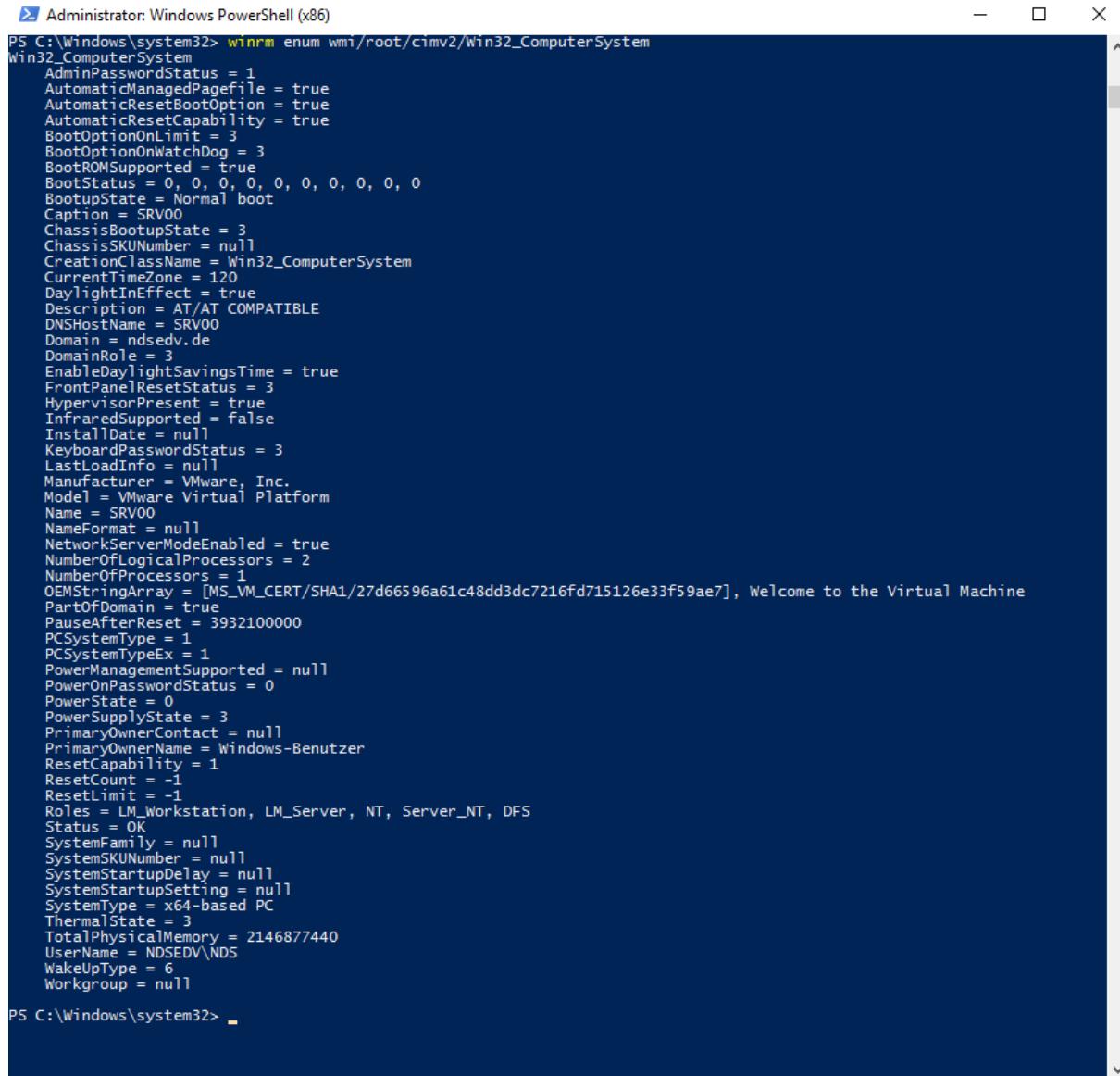
```
Administrator: Windows PowerShell (x86)
PS C:\Windows\system32> winrm e winrm/config/listener
Listener [Source="GPO"]
  Address = *
  Transport = HTTP
  Port = 5985
  Hostname
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint
  ListeningOn = 127.0.0.1, 172.18.32.110, ::1, fe80::5efe:172.18.32.110%3

Listener [Source="Compatibility"]
  Address = *
  Transport = HTTPS
  Port = 443
  Hostname = SRV00.ndsedv.de
  Enabled = true
  URLPrefix = wsman
  CertificateThumbprint = b5 40 a4 50 9e e8 a8 17 66 29 30 9c 16 02 7f ac5b b2 b3 d4
  ListeningOn = 127.0.0.1, 172.18.32.110, ::1, fe80::5efe:172.18.32.110%3
PS C:\Windows\system32>
```



Windows Admin Center – Honolulu installieren

WINRM Kommunikation zum lokalen WMI testen:



```
Administrator: Windows PowerShell (x86)
PS C:\Windows\system32> winrm enum wmi/root/cimv2/Win32_ComputerSystem
Win32_ComputerSystem
AdminPasswordStatus = 1
AutomaticManagedPagefile = true
AutomaticResetBootOption = true
AutomaticResetCapability = true
BootOptionOnLimit = 3
BootOptionOnWatchDog = 3
BootROMSupported = true
BootStatus = 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
BootupState = Normal boot
Caption = SRV00
ChassisBootupState = 3
ChassisSKUNumber = null
CreationClassName = Win32_ComputerSystem
CurrentTimeZone = 120
DaylightInEffect = true
Description = AT/AT COMPATIBLE
DNSHostName = SRV00
Domain = ndsedv.de
DomainRole = 3
EnableDaylightSavingsTime = true
FrontPanelResetStatus = 3
HypervisorPresent = true
InfraredSupported = false
InstallDate = null
KeyboardPasswordStatus = 3
LastLoadInfo = null
Manufacturer = VMware, Inc.
Model = VMware Virtual Platform
Name = SRV00
NameFormat = null
NetworkServerModeEnabled = true
NumberOfLogicalProcessors = 2
NumberOfProcessors = 1
OEMStringArray = [MS_VM_CERT/SHA1/27d66596a61c48dd3dc7216fd715126e33f59ae7], Welcome to the Virtual Machine
PartOfDomain = true
PauseAfterReset = 3932100000
PCSystemType = 1
PCSystemTypeEx = 1
PowerManagementSupported = null
PowerOnPasswordStatus = 0
PowerState = 0
PowerSupplyState = 3
PrimaryOwnerContact = null
PrimaryOwnerName = Windows-Benutzer
ResetCapability = 1
ResetCount = -1
ResetLimit = -1
Roles = LM_Workstation, LM_Server, NT, Server_NT, DFS
Status = OK
SystemFamily = null
SystemSKUNumber = null
SystemStartupDelay = null
SystemStartupSetting = null
SystemType = x64-based PC
ThermalState = 3
TotalPhysicalMemory = 2146877440
UserName = NDSEDV\NDS
WakeUpType = 6
Workgroup = null
PS C:\Windows\system32> -
```

Firewall Port für https setzen:

```
netsh advfirewall firewall add rule name="Windows Remote Management (HTTPS-In)" protocol=TCP dir=in localport=5986 action=allow
```

```
New-NetFirewallRule -DisplayName "Windows Remote Management (HTTPS-In)" -Name "Windows Remote Management (HTTPS-In)" -Profile Any -LocalPort 5986 -Protocol TCP
```

```
netsh advfirewall firewall set rule group="Remote Administration" new enable=yes
netsh advfirewall firewall set rule group="Windows Remote Management" new enable=yes
netsh advfirewall firewall set rule group="Windows Management Instrumentation (wmi)" new enable=yes
```

Firewall Regeln abfragen:

```
Get-NetFirewallRule WINRM-HTTP-In-TCP* | fl Name, DisplayName, Enabled
Test-NetConnection -computername SRV01 -port 3389
Test-NetConnection -computername SRV01 -CommonTCPPort RDP
```



Windows Admin Center – Honolulu installieren

WINRM Kommunikation zu Remote Server WMI testen:

```
Administrator: Windows PowerShell (x86)
PS C:\Windows\system32> winrm enum wmi/root/cimv2/Win32_ComputerSystem -r:IssuingCA
Win32_ComputerSystem
AdminPasswordStatus = 1
AutomaticManagedPagefile = true
AutomaticResetBootOption = true
AutomaticResetCapability = true
BootOptionOnLimit = 3
BootOptionOnWatchDog = 3
BootROMSupported = true
BootStatus = 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
BootupState = Normal boot
Caption = ISSUINGCA
ChassisBootupState = 3
ChassisSKUNumber = null
CreationClassName = Win32_ComputerSystem
CurrentTimeZone = 120
DaylightInEffect = true
Description = AT/AT COMPATIBLE
DNSHostName = IssuingCA
Domain = ndsedv.de
DomainRole = 3
EnableDaylightSavingsTime = true
FrontPanelResetStatus = 3
HypervisorPresent = true
InfraredSupported = false
InstallDate = null
KeyboardPasswordStatus = 3
LastLoadInfo = null
Manufacturer = VMware, Inc.
Model = VMware Virtual Platform
Name = ISSUINGCA
NameFormat = null
NetworkServerModeEnabled = true
NumberOfLogicalProcessors = 2
NumberOfProcessors = 1
OEMStringArray = [MS_VM_CERT/SHA1/27d66596a61c48dd3dc7216fd715126e33f59ae7], Welcome to the Virtual Machine
PartOfDomain = true
PauseAfterReset = 3932100000
PCSystemType = 1
PCSystemTypeEx = 1
PowerManagementSupported = null
PowerOnPasswordStatus = 0
PowerState = 0
PowerSupplyState = 3
PrimaryOwnerContact = null
PrimaryOwnerName = Windows-Benutzer
ResetCapability = 1
ResetCount = -1
ResetLimit = -1
Roles = LM_Workstation, LM_Server, NT, Server_NT
Status = OK
SystemFamily = null
SystemSKUNumber = null
SystemStartupDelay = null
SystemStartupSetting = null
SystemType = x64-based PC
ThermalState = 3
TotalPhysicalMemory = 2146877440
UserName = NDSEDV\NDS
WakeUpType = 6
Workgroup = null
PS C:\Windows\system32> -
```

WinRM Schnellkonfiguration:

```
winrm quickconfig -transport:https
Enable-PSRemoting
```

WinRM Remote Konfiguration:

```
psexec \\ComputerName -s winrm.cmd quickconfig -q
psexec @c:\PCs.txt -s winrm.cmd quickconfig -q
winrm get wmicimv2/Win32_Service?Name=WinRM -r:SRV00
```



Windows Admin Center – Honolulu installieren

HTTPS Listener einrichten:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS
@{Hostname="WindowsAdminCenter";
CertificateThumbprint="93ed28bb2d9d15f9cb80a8ab82c7bb1325e731e5"}
```

```
Set-WsmanQuickConfig -UseSSL
```

HTTPS Listener löschen:

```
winrm delete winrm/config/Listener?Address=*+Transport=http
```

Remote Port testen:

```
Test-NetConnection -ComputerName SRV00 -Port 5986
```

Remote Verbindung aufbauen:

```
Enter-PSSession -ComputerName SRV00
```

```
$options=New-PSSessionOption -SkipCACheck -SkipCNCheck
Enter-PSSession -ComputerName SRV00-Credential NDS -UseSSL -SessionOption
$options
```

Zertifikat zuweisen:

```
winrm set winrm/config/service
@{CertificateThumbprint="93ed28bb2d9d15f9cb80a8ab82c7bb1325e731e5"}
```

Alle Zertifikate auslesen:

```
Get-ChildItem -Path cert: -Recurse | select Subject, FriendlyName, Thumbprint | Format-List
```

Alle lokalen Computerzertifikate auslesen:

```
Get-ChildItem -path cert:\LocalMachine\My
```



Windows Admin Center – Honolulu installieren

Lokale Port WSMAN auslesen:

```
Get-ChildItem WSMan:\localhost\Client\DefaultPorts
```

WSManConfig: Microsoft.WSMAN.Management\WSMan::localhost\Client\DefaultPorts			
Type	Name	SourceOfValue	Value
System.String	HTTP		5985
System.String	HTTPS		5986

WSMan prüfen:

```
Test-WSMan -Computername IssuingCA -UserSSL  
"DC01","DC022" | foreach{$_; Test-WsMan $_}
```

```
Administrator: Windows PowerShell  
PS C:\Windows\system32> Test-WSMan -Computername IssuingCa.ndsedv.de  
  
wsmid      : http://schemas.dmtf.org/wbem/wsman/identity/1/wsmanidentity.xsd  
ProtocolVersion : http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd  
ProductVendor  : Microsoft Corporation  
ProductVersion : OS: 0.0.0 SP: 0.0 Stack: 3.0  
  
PS C:\Windows\system32> Test-WSMan -Computername IssuingCa.ndsedv.de -UseSSL  
  
wsmid      : http://schemas.dmtf.org/wbem/wsman/identity/1/wsmanidentity.xsd  
ProtocolVersion : http://schemas.dmtf.org/wbem/wsman/1/wsman.xsd  
ProductVendor  : Microsoft Corporation  
ProductVersion : OS: 0.0.0 SP: 0.0 Stack: 3.0  
  
PS C:\Windows\system32>
```

Powershell Berechtigungen auslesen:

```
(Get-PSSessionConfiguration -Name Microsoft.PowerShell).Permission  
(Get-PSSessionConfiguration -Name "Microsoft.PowerShell").SecurityDescriptorSDDL
```

Berechtigungen hinzufügen:

```
net localgroup "Remote Management Users" /add Joern  
Set-PSSessionConfiguration -Name Microsoft.PowerShell -showSecurityDescriptorUI
```

Berechtigungen anhand des SDDL Strings setzen:

```
(Get-PSSessionConfiguration -Name "Microsoft.PowerShell").SecurityDescriptorSDDL
```

```
Set-PSSessionConfiguration -Name Microsoft.PowerShell -SecurityDescriptorSddl $SDDL
```

```
$SDDL =  
O:NG:BAD:P(A;;GA;;;BA)(A;;GA;;;IU)(A;;GA;;;RM)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW  
;;;WD)
```



Windows Admin Center – Honolulu installieren

Vertrauensstellung:

```
winrm set winrm/config/client/auth '@{Basic="true"}'  
winrm set winrm/config/service/auth '@{Basic="true"}'  
winrm set winrm/config/service '@{AllowUnencrypted="true"}'
```

Domänen-Vertrauensstellung testen:

```
$Credential = Get-Credential  
Test-ComputerSecureChannel -Repair -Credential $Credential  
Reset-ComputerMachinePassword
```

WINRM komplette lokale Konfiguration CMD:

```
winrm quickconfig -q  
winrm set winrm/config/winrs '@{MaxMemoryPerShellMB="512"}'  
winrm set winrm/config '@{MaxTimeoutms="1800000"}'  
winrm set winrm/config/service '@{AllowUnencrypted="true"}'  
winrm set winrm/config/service/auth '@{Basic="true"}'
```

```
Start-Service WinRM  
SetService WinRM -StartupType Automatic  
Set-ExecutionPolicy Unrestricted
```

WINRM komplette lokale Konfiguration Powershell:

```
# Rückbau > Deaktivieren  
  
Start-Service winrm  
winrm invoke restore winrm/config  
Disable-PSRemoting -Force  
Disable-WSManCredSSP -Role Client  
Disable-WSManCredSSP -Role Server  
Stop-Service winrm  
  
# Aufbau > Aktivieren  
  
Enable-PSRemoting -Force  
Enable-WSManCredSSP -Role Server -Force  
Enable-WSManCredSSP -Role Client -DelegateComputer "*" -Force  
winrm enumerate winrm/config/listener
```

Selbstsigniertes Zertifikat erstellen und Listener setzen:

```
$c = New-SelfSignedCertificate -DnsName "SRV00.ndsedv.de" -CertStoreLocation  
cert:\LocalMachine\My  
  
winrm create winrm/config/Listener?Address=*+Transport=HTTPS "@{Hostname='`"  
SRV00.ndsedv.de`"';CertificateThumbprint='`"$(($c.ThumbPrint)`"')`"}"
```

Remote Desktop Connection abfragen:

```
Get-ItemProperty "HKLM:\System\CurrentControlSet\Control\Terminal Server" -name  
"fDenyTSConnections" | fl fDeny*  
  
Set-ItemProperty "HKLM:\System\CurrentControlSet\Control\Terminal Server" -name  
"fDenyTSConnections" -value 0
```



Windows Admin Center – Honolulu installieren

WSMAN SPN setzen:

```
Setspn -L ndsedv.de\SRV00
Setspn -A WSMAN\SRV00 ndsedv.de\SRV00
Setspn -A WSMAN\SRV00.ndsedv.de ndsedv.de\SRV00
```

Fehlermeldungen analysieren:

winrm helpmsg 0x80338104

HKEY_CLASSES_ROOT (2147483648 (0x80000000))
HKEY_CURRENT_USER (2147483649 (0x80000001))
HKEY_LOCAL_MACHINE (2147483650 (0x80000002))
HKEY_USERS (2147483651 (0x80000003))
HKEY_CURRENT_CONFIG (2147483653 (0x80000005))
HKEY_DYN_DATA (2147483654 (0x80000006))

<https://msdn.microsoft.com/en-us/library/aa394559%28VS.85%29.aspx>

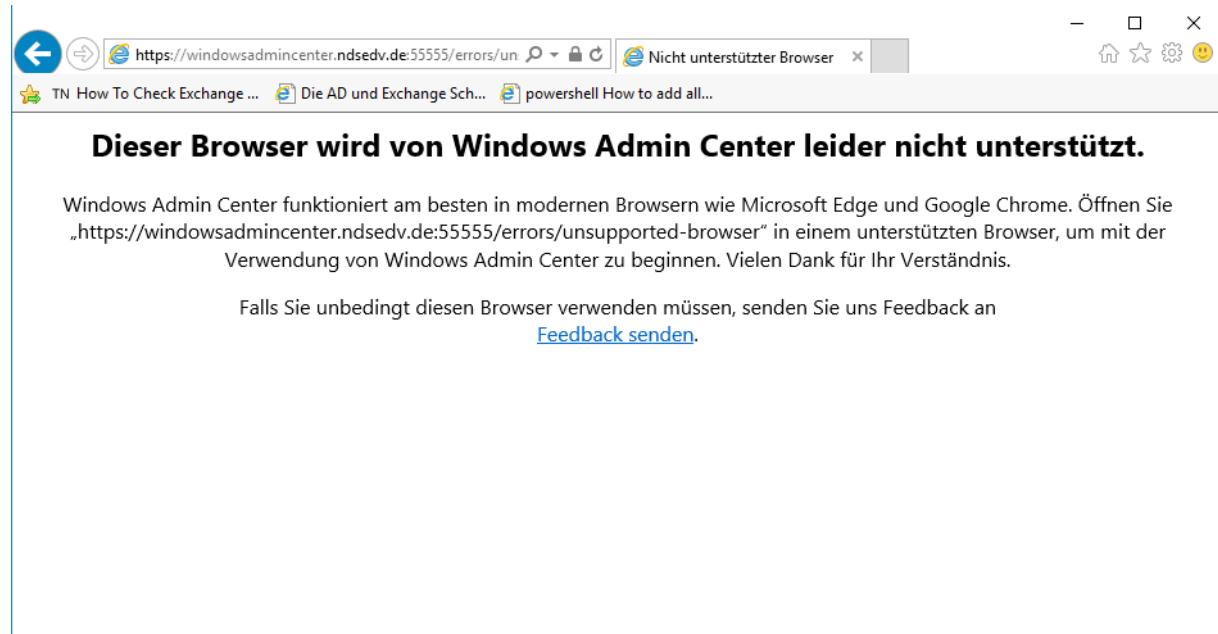
TLS Unterstützung Windows Systeme:

Windows OS Version	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2
Windows XP & Windows Server 2003	✓	✓	✓	✗	✗
Windows Vista & Windows Server 2008	✓	✓	✓	✓	✓
Windows 7 & Windows Server 2008 R2	✓	✓	✓	✓	✓
Windows 8 & Windows Server 2012	✓	✓	✓	✓	✓
Windows 8.1 & Windows Server 2012 R2	✓	✓	✓	✓	✓
Windows 10 & Windows Server 2016	✓	✓	✓	✓	✓



Windows Admin Center – Honolulu installieren

Internet Explorer nicht unterstützter Browser:



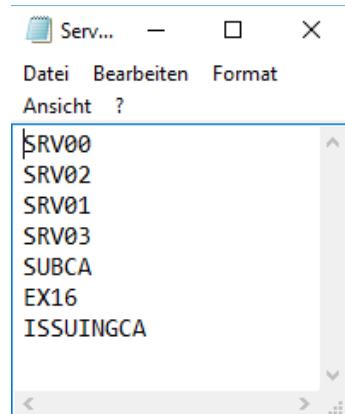
Dieser Browser wird von Windows Admin Center leider nicht unterstützt.

Windows Admin Center funktioniert am besten in modernen Browsern wie Microsoft Edge und Google Chrome. Öffnen Sie „<https://windowsadmincenter.ndsedv.de:55555/errors/unsupported-browser>“ in einem unterstützten Browser, um mit der Verwendung von Windows Admin Center zu beginnen. Vielen Dank für Ihr Verständnis.

Falls Sie unbedingt diesen Browser verwenden müssen, senden Sie uns Feedback an [Feedback senden](#).

Serverliste für den Import erstellen:

```
Get-ADComputer -SearchBase "OU=Server,OU=Machines,OU=ORG,DC=ndsedv,DC=de" -Filter "*" | %{$_.Name} | Out-File -FilePath C:\Temp\Server.txt -Append }
```



SRV00
SRV02
SRV01
SRV03
SUBCA
EX16
ISSUINGCA