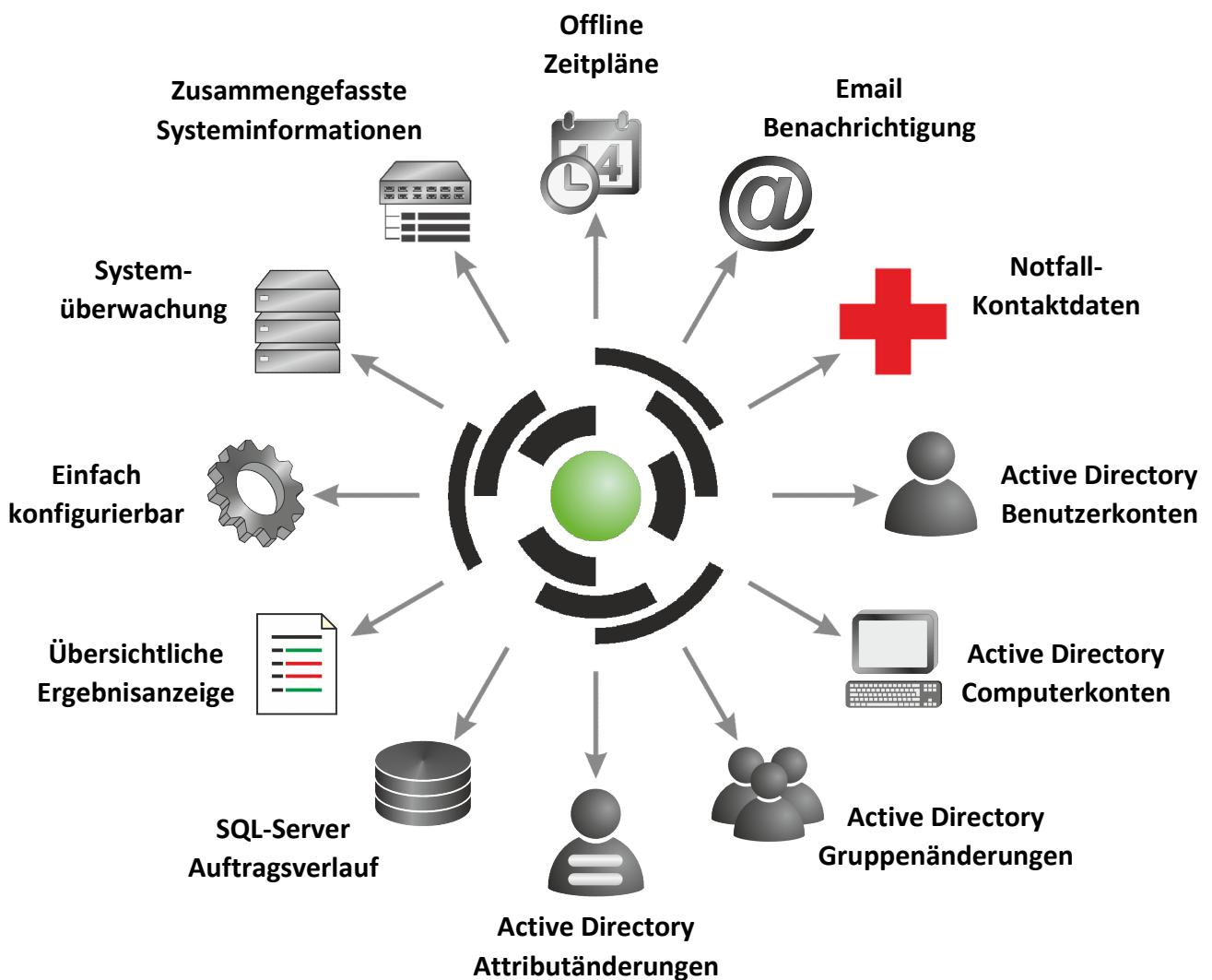




# Systemüberwachung

Einfach – Schnell – Universell





Im Gegensatz zu herkömmlichen Überwachungslösungen ergänzt node**WATCH** die Geräteüberwachung zusätzlich um die Möglichkeit der Überwachung von Active-Directory Objekten. Ob fehlende Netzwerkverfügbarkeit, abgelaufene Kennwörter, gesperrte Benutzerkonten, geänderte Gruppenmitgliedschaften, node**WATCH** entgeht nichts!

## Einfach

in der Bedienung

## Schnell

Konfiguriert

## Universell

in der Überwachung





## Systemüberwachung



Die Überwachungsmöglichkeiten richten sich nach dem jeweiligen Endgerät. Folgende Überwachungen sind möglich:

- Windows Endgeräte:
- ▶ Pingbarkeit
  - ▶ Port Scan auf offene Ports
  - ▶ freier Festplattenspeicher
  - ▶ Laufende Dienste,
  - ▶ laufende Prozesse
  - ▶ Fehlereinträge in EventLog Protokolle

- Sonstige Endgeräte:
- ▶ Pingbarkeit
  - ▶ Port Scan auf offene Ports
  - ▶ SNMP Abfragen

Nach Klick auf die überwachte Node sieht man sofort eine zusammengefasste Ergebnisübersicht der Überwachung. Ein Klick auf einen Ergebniseintrag öffnet die Details zur Überwachung.

SAPDEV	Passau	Disk	Größe	Belegt	Frei	Grenze1	Grenze2	DS
10.0.1.32	Server Virtuell	C:	100 GB	24 GB	76 GB (76 %)	10 %	5 GB	NTFS
<b>Kritisches System</b>		D:	30 GB	30 GB	0 GB (0,0 %)	10 %		NTFS
SAP Testsystem		E:	50 GB	26 GB	24 GB (48 %)	10 %	5 GB	NTFS
		F:	60 GB	20 GB	40 GB (66 %)	10 %	5 GB	NTFS
X Ping	07.03.2019 14:57:37	G:	1200 GB	421 GB	779 GB (65 %)	10 %	5 GB	NTFS
Port	-	H:	500 GB	302 GB	198 GB (40 %)	10 %	5 GB	NTFS
X Disk	07.03.2019 14:57:37							
X Service	07.03.2019 14:57:37							
X EventLog	07.03.2019 14:57:38							
X Process	07.03.2019 14:57:38							
SNMP	-							



Die runden Buttons ermöglichen einen schnellen Zugriff auf Geräteinformationen, Überwachungsprotokoll, Neustart von Windows Endgeräten, Bearbeitung der Überwachungseinstellungen sowie Notfallinformationen.



## Systemübersicht



Zusammenfassung wichtiger Informationen von Windows-Endgeräten oder SNMP-fähigen Endgeräten.

**SRVHR1** [Schließen]

Benutzer: Keine lokale Anmeldung

Benutzer (RDP-Anmeldung)	Startzeit
NODEWATCH\Netzadmin	25.02.2019 09:36:08

Hersteller: Dell Inc.  
Seriennummer: BCZQWX1  
UUID: 4C4C4544-0043-5A10-8051-C2C04F575831  
Name: PowerEdge R420

CPU: Intel(R) Xeon(R) CPU E5-2440 0 @ 2.40GHz  
RAM (total / used / free): 128 GB / 67,3 GB / 60,7 GB  
Slots: 12 (16)(16)(-)(16)(16)(-)(16)(16)(-)(-)

RunTime: Tage: 8 Stunden: 6 Minuten: 19 (seit: 25.02.2019 09:34)

Bios: Phoenix ROM BIOS PLUS Version 1.10 2.1.3  
OS: Microsoft Windows Server 2012 R2 Standard (64-Bit) - (9600)  
Aktive Prozesse: 103

Drive	Boot	Size	Used	Usage	Free	Type	Filesystem
C:	*	132,7 GB	73,7 GB	<div style="width: 55%;"></div>	59,0 GB	Lokale Festplatte	(NTFS)
D:		703,8 GB	545,2 GB	<div style="width: 77%;"></div>	158,6 GB	Lokale Festplatte	(NTFS)
E:		0,0 GB	0,0 GB	<div style="width: 0%;"></div>	0,0 GB	CD	

Adapter	MAC	IP	Mask
Standard GW	90:B1:1C:41:94:84	172.16.1.6	
		172.16.254.254	

Name	DisplayName	Pfad	Caption	Description	ErrorCr	Process
AdobeARMServ...	Adobe Acrobat...	...C:\Program...	Adobe Acro...	Adobe Acro...	Ignore	1880

**Drucker IT** [Schließen]

UTAX TA Printing System

Drucker II / 1/2.16.2.58

Modellinfo	Standort:	Buero IT
	Modell:	P-3521UN
	Seriennummer:	LYD5516078

Gerätestatus	System:	2P1_3F00.003.204
	Maschine:	2P1_1000.002.001
	Displaytext:	Ruhemodus

Netzwerk	IP-Adresse:	172.16.2.58
	Subnet-Mask:	255.255.0.0
	DNS1:	10.0.1.1
	DNS2:	10.0.1.2
	MAC:	00 17 C8 1D E6 58

Toner	Schwarz:	83 %	voll
-------	----------	------	------

Zähler	A4:	3328
	B5:	0
	A5:	6
	Folio:	0
	Legal:	0
	Letter:	0
	Statement:	0
	Other1:	0
	Other2:	0
	Seiten Total:	3334

## Offline Zeitpläne



Erstellen Sie für offline Zeitpläne um die Überprüfung von Endgeräten außerhalb der Arbeitszeit auszusetzen, oder definieren Sie einen Zeitplan für Wartungsarbeiten. Je Endgerät kann ein individueller offline Zeitplan zugeordnet werden.

**Zeitplan - Prüffreie Zeit**

**Zeitplan einstellen** [OK]

**Häufigkeit:**

**Wochentag** (ausgewählt)

- Monat: Erster
- Monat: Zweiter
- Monat: Dritter
- Monat: Vierter
- Monat: Letzter
- Tag im Monat

Montag

Dienstag

Mittwoch

Donnerstag

Freitag

Samstag

Sonntag

**Beginnt am:** 01.01.2017

**Endet am:** 31.12.2199

**Startzeit:** 00:00

**Endzeit:** 23:59



## Benachrichtigung



Automatische Email-Benachrichtigung im Fehlerfall. Zusammenfassung von Fehlermeldungen in einer Benachrichtigungsmail z.B. 60 Sekunden sammeln. Je überwachtes Gerät individuelle Empfänger einstellbar.

## Notfallkontaktdaten



Ermöglicht die Verwaltung von Vertragsdaten und Notfallansprechpartner, so dass im Notfall alle wichtigen Daten sofort zur Hand sind.

Vertragsdaten

**SRVHR1**

P&I Loga Systempartner  
- vom 07.09.2005 - - ak12344 -

5

Vertragspartner Systempartner  
Systempartner

Straße Musterstrasse 1

Land / PLZ / Ort DE 99999 Musterhausen

ServiceLevel 5/24 - 48

Kundnummer 712377

Vertragsnummer ak12344

Vertragsbeginn 01.04.2017

Vertragsende 31.12.9998

Notfall Hotline +49 9999 / 999 - 999

Service-Portal

Benutzername

Passwort

Bemerkungen  
Wenn die Störung an einem Werktag bis spätestens 12:00 gemeldet wird, dann erfolgt die Reaktionszeit bis spätestens 16:30 des darauf folgenden Werktags.

Zuordnen Ändern Entfernen Erstellen Schliessen

## Active-Directory Computerkonten



Spüren Sie veraltete Computerkonten-Einträge im Active Directory auf und räumen Sie auf. Überwachen Sie folgende Active-Directory Computerkonteneigenschaften:

- ▶ veraltete Konten
- ▶ deaktivierte Konten



## Active-Directory Benutzerkonten



Spüren Sie veraltete Benutzerkonten-Einträge im Active-Directory auf und räumen Sie auf. Lassen Sie sich zusammengefasste Informationen von auffälligen Objekten anzeigen. Überwachen Sie folgende Active-Directory Benutzerkonteneigenschaften:

- ▶ gesperrte Konten
- ▶ abgelaufene oder bald ablaufende Konten
- ▶ veraltete Konten
- ▶ deaktivierte Konten
- ▶ Konten, die gegen Kennwortrichtlinien verstoßen

Sie können sich in jeder Benutzerauflistung die wichtigsten Details eines Benutzerkontos anzeigen lassen. Ein Register zeigt alle relevanten Kontaktinformationen, der andere alle gängigen Sicherheitseinstellungen.

The screenshot shows the 'Active Directory Objektinfo' window for user 'Teichmann Emil'. The window is divided into several sections:

- Beschreibung:** Dies ist eine nodeWATCH Testbenutzer!
- Kontakt Info:** Contains fields for Anmeldename (TeichmannE), UPN (TeichmannE@nodewatch.de), cn (Teichmann Eva), Name (Teichmann Eva), GUID (6fe743966bd80e4f83995eb137448e0e), homeDrive, homeDirectory, profilePath (\\nas1\profile\$\TeichmannE), scriptPath (LOGIN.bat), and SID (S-1-5-21-906218691-1799505843-967687043-14208).
- Member Of:** Lists groups such as Domänen-Benutzer (Primary Group), GA\_Produkmappe\_Schriftverkehr, GA\_Praesentationen, GA\_Angebotsverwaltung\_SAP\_Andern, GS\_DSB\_Infoboard\_Administratoren, GV\_Einkauf, GS\_ELM\_Archiv\_7T, GS\_Internet\_Benutzer, GA\_Belegverwaltung\_Lesen, and GS\_Materialwirtschaft.
- Anmelden an:** Lists servers PCAZB11, PCCAD14, and PCEMPFANG.
- Anmeldezeitbeschränkung:** A calendar grid showing login restrictions for days of the week and hours of the day.
- Veraltet:** lastLogon (05.10.2018 12:18:20), LogonDC (DCBUCT LLTS), logonCount (39), whenCreated (13.08.2018 07:26:55).
- Kennwort abgelaufen:** pwdLastSet (21.11.2018 13:09:28), pwdAge (76), badPwdTime (19.09.2018 15:26:03), badPwdCount (0).
- Password Policy:** Includes fields for Kennwortalter (0-60), Passwortlänge (8), Kennwort Historie (12), Sperrdauer (60), Anzahl Versuche (5), and a checked 'Komplexität' checkbox.
- Konto ist gesperrt:** Includes checkboxes for 'Bei nächster Anmeldung Kennwortände', 'Kann Kennwort nicht ändern', and 'Kennwort läuft nie ab'.
- Account abgelaufen:** Checked checkbox with 'läuft ab am' (20.10.2018).
- Konto deaktiviert:** Unchecked checkbox.

At the bottom, the distinguishedName is shown as CN=Teichmann Eva,OU=Praktikanten,OU=Obernzell,DC=nodewatch,DC=de, and a 'Schließen' button is present.



## Active-Directory Gruppen



Überwachen Sie Änderungen an Active-Directory Gruppenmitgliedschaften. Bestätigen Sie die Mitglieder von sensiblen Gruppen wie Domänen-Administratoren oder selbst erstellte Sicherheitsgruppen für z.B. Personalwesen und lassen Sie sich Mitgliedsänderungen aktiv anzeigen. Sind die Änderungen OK, dann bestätigen Sie diese einfach.

Es kann eine beliebige Anzahl von Gruppen in drei verschiedene Kategorien unterteilt werden, wie z.B. Administrative Gruppen, Kritische Anwendungsgruppen, sonstige Gruppen, die überwacht werden sollen.

DisplayName	Beschreibung	Unbestätigt
<b>Admin Groups</b>	Gruppen mit Administrativen Berechtigungen	<b>2</b>
<b>Kritische Anwendungen</b>	Gruppen mit Zugriff auf kritische Anwendungen	<b>0</b>
<b>Sonstige kritische Gruppen</b>	Gruppen mit Zugriff auf kritische Dateien ...	<b>0</b>

Name	Members	OK ?	Changed
Schema-Admins	3	1	07.03.2019
Sicherungs-Operatoren	1	1	07.03.2019

Gültig	Info	DisplayName	Created	Changed
<input checked="" type="checkbox"/>		Netzadmin	28.01.2005	07.03.2019
<input checked="" type="checkbox"/>		Notfalladmin	31.03.2004	07.03.2019
<input type="checkbox"/>		Schuwa	22.01.2013	07.03.2019

Name	membe	Erstellt
_Gruppe_Saperion_ELM		07.02.2007
Abgelehnte RODC-Kennwortreplikationsgruppe		07.02.2013
Administratoren	Admin	31.03.2004
Benutzer	Builti...	31.03.2004
Delegated Setup		30.07.2013
DHCP-Administratoren		31.03.2004
DHCP-Benutzer		31.03.2004
Discovery Management		30.07.2013
Distributed COM-Benutzer	Builti...	12.03.2008
DnsAdmins		31.03.2004
DnsUpdateProxy		31.03.2004
Domänen-Admins	Admin	31.03.2004

Buttons: Abbruch, Überprüfung durchführen, Ok

Werden neue Benutzerkonten zu überwachten Gruppen hinzugefügt, dann wird dieses im Überwachungsmodus angezeigt.



Mit Klick auf das Überwachungssymbol gelangt man sofort zum Detail!



## Active-Directory Benutzerkontenänderungen

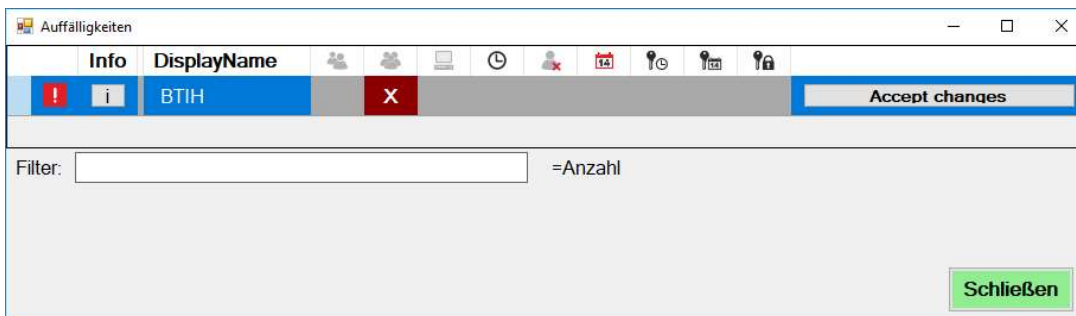


Gruppen-Benutzerkonten, die von mehreren Personen gleichzeitig verwendet werden, bedürfen besonderer Aufmerksamkeit. Zusätzliche Gruppenmitgliedschaften in solchen Konten berechtigen alle Nutzer dieses Kontos für die neuen Sicherheitseinstellungen.

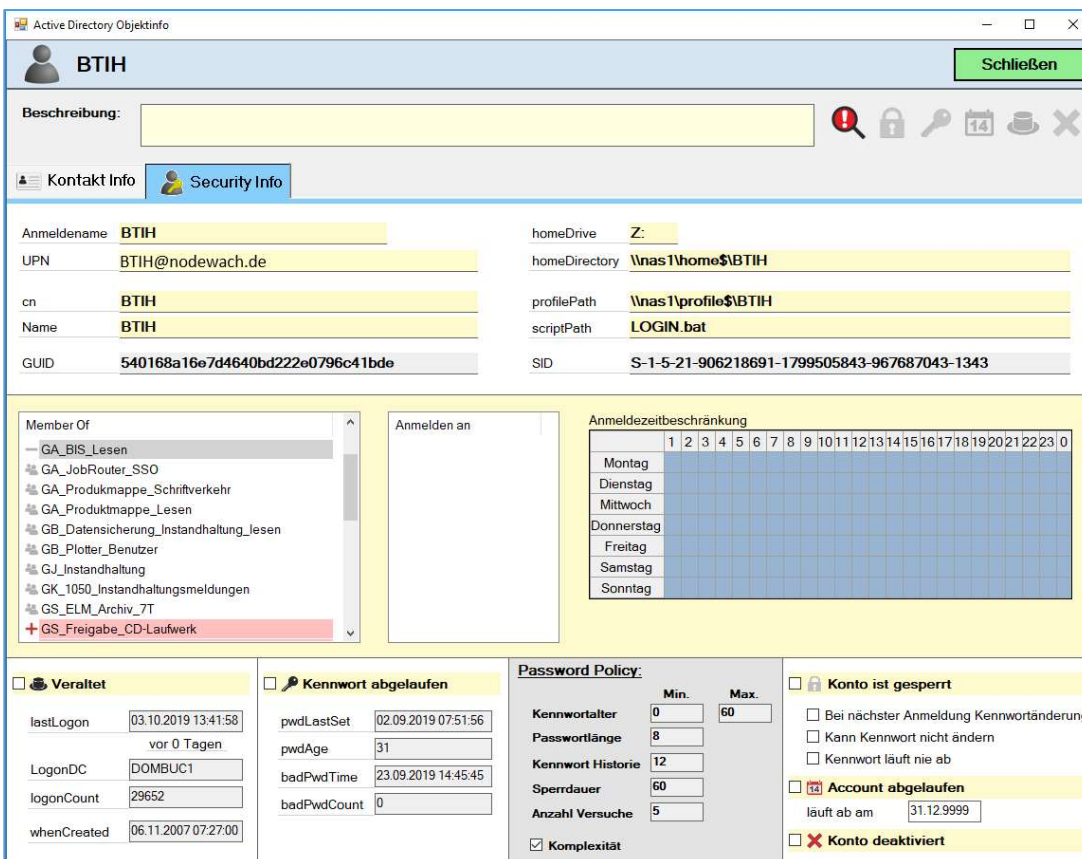
Überwachen Sie Änderungen an Sicherheitsrelevanten Attributen wie...

- ▶ Kennworteinstellungen
- ▶ Arbeitsstationsbeschränkungen
- ▶ Anmeldezeiten
- ▶ Gruppenmitgliedschaften

In der Detailansicht werden die Änderungen rot hervorgehoben!



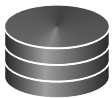
Nach Klick auf den Info-Button erscheinen die zusätzlichen Einträge in rot.







## SQL-Server Auftragsverlauf



Überwachen Sie den Auftragsverlauf von beliebig vielen Microsoft SQL-Servern und lassen Sie sich fehlgeschlagene Auftragschritte schnell und einfach anzeigen.

Protokoll - □ ×

**Letzte Prüfung: 07.03.2019 02:50:20**

Prüfergebnis für

**SQL-Task Fehler**

---

S... Prüfgegenstand

- ✓ SRV38 - ECA03360-38A8-4B0B-9E74-35CADFFFC66A --> Erfolg
- ✓ SRV38 - JobRouter\_Ausschussgrund\_Massnahmen --> Erfolg
- ✓ SRV38 - Interation\_Produktivität --> Erfolg
- ✓ SRV38 - SLS\_Lagerstamm\_Update --> Erfolg
- ✓ SRV38 - Produktionsplanung\_Datenimport --> Erfolg
- ✓ SRV38 - Integration\_Export\_AuftragsplanungBauer --> Erfolg
- ✓ SRV38 - Datensicherung.Subplan\_1 --> Erfolg
- ✓ SRV38 - syspolicy\_purge\_history --> Erfolg
- ✓ SRV38 - Daten\_SAP\_Import --> Erfolg
- ✗ SRV42 - Sicherung.Subplan\_1 --> Error
- ✓ SRV42 - Belastungen\_Aktualisierung --> Erfolg
- ✓ SRV42 - syspolicy\_purge\_history --> Erfolg
- ✗ SRV42 - Nachlauf\_Automatisierungen --> Error

---

<Fehler>	7..	ActiveDirectory <== Telefonanlage
Erfolg	6..	Telefonliste_im_HTML_Format_Aufbereiten
Erfolg	5..	Dienstbenutzer_in_Active_Directory_eintragen
Erfolg	4..	Active_Directory_User_Kennzeichen
Erfolg	3..	Active Directory Beschreibung übertragen
Erfolg	2..	Nachlauf
<Fehler>	1..	Telefonanlage_Datenimport

**Schließen**



# Überwachungsprotokoll



Am Ende einer Überwachung werden die Ergebnisse der Überwachung übersichtlich zusammengefasst.

Überwachungsprotokoll

## SAPDEV

- Statusprotokoll
- Notfallkontakt
- Systeminfo

ScopeText	DateTime
✓ Ping	07.03.2019 14:44
✓ Disk	07.03.2019 14:44
✓ Service	07.03.2019 14:44
⚠ EventLog	07.03.2019 14:44
✓ Process	07.03.2019 14:44

Object
✓ C: Freier Speicher 76,22 %
✓ E: Freier Speicher 47,74 %
✓ F: Freier Speicher 66,15 %
✓ G: Freier Speicher 64,96 %
✓ H: Freier Speicher 39,63 %

### Teilergebnisse der Prüfung

Stat	Subject	Value1	Value2	Value3	Value4	Value5	Value6
1	✓ C:	100 GB	24 GB	76 GB (76 %)	10 %	5 GB	NTFS

1

### Detail

Laufwerk: C:  
Dateisystem: NTFS  
Größe: 100 GB  
Belegt: 24 GB

Frei: 76 GB

Freier Speicher in Prozent: 76,22 %

Meldung ab Schwellenwert: 5,00 GB

**Schliessen**



## Einfache Konfiguration



In der Erstkonfiguration können sie einfach über einen Active-Directory Scan alle Windows Endgeräte mit einer Standardkonfiguration zur Überwachung hinzufügen. Außerdem können Sie mittels Broadcast-Ping das Netzwerk nach weiteren Geräten durchsuchen.

Die Detailkonfiguration kann dann in der Überwachung eingerichtet werden. Zu überwachende Werte auswählen, Schwellenwert einstellen, fertig!

Node bearbeiten

SAPDEV Schließen

NodeInfo WMI Settings SNMP Verträge

WMI Unterstützung

Anmeldeinfo: Standard

**Laufwerksüberwachung**

Aktiv	Disk	Ausschluss	Grenze1	GE	Grenze2	GE
<input checked="" type="checkbox"/>	*	<input type="checkbox"/>	10,00	%	5,00	GB
<input checked="" type="checkbox"/>	D:	<input checked="" type="checkbox"/>	0,00	%	0,00	%

Select

**Dienstüberwachung**

Aktiv	Dienstname	Beschreibung
<input checked="" type="checkbox"/>	SAPDEV_00	SAPDEV_00
<input checked="" type="checkbox"/>	SAPDEV_01	SAPDEV_01
<input checked="" type="checkbox"/>	SAPHostControl	SAPHostControl

Select

**EventLog Fehler überwachen**

Aktiv	Protokoll	WALd	Events
<input checked="" type="checkbox"/>	System	Error	Events
<input checked="" type="checkbox"/>	Application	Error	Events

Select

**Aktive Prozesse überwachen**

Aktiv	ProcessName	Proz.Aktiv	Kill	Beschreib
<input checked="" type="checkbox"/>	dwm.exe	<input type="checkbox"/>	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	sqlservr.exe	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>	

Select

Bevor Sie mit der Einrichtung der Überwachung beginnen, wählen Sie unter Anmeldeinfo ein Konto aus, das ausreichende Berechtigung für das zu überwachende System besitzt. Bei Standardeinstellung wird das in den Basiseinstellungen hinterlegte Konto verwendet.

Um die Überwachung einzurichten, tippen Sie unter der gewünschten Überwachung einfach auf den Select-Button. Wählen Sie dann in dem darauf folgenden Fenster die zu überwachenden Objekte aus. Legen sie bei Bedarf noch den gewünschten Schwellenwert für die Überwachung fest.

Überwachung

Drive	Size	Free	% Free	Volume Name
Default				
<input checked="" type="checkbox"/>	*			
<input type="checkbox"/>	C:	99.656	75.962	76 %
<input checked="" type="checkbox"/>	D:	29.997	0.005	0 % SWAP
<input type="checkbox"/>	E:	49.997	23.867	48 % EKE
<input type="checkbox"/>	F:	59.997	39.686	66 % LOGS
<input type="checkbox"/>	G:	1199.997	779.484	65 % DATA
<input type="checkbox"/>	H:	499.997	198.157	40 % ARCH

Ok Abbruch



## Die Überwachung



In der Überwachungssicht werden alle Nodes nach Standort und Gruppierung angezeigt. Prüfkategorien und Ergebnis der Prüfung sind sofort erkennbar. Durch Klick auf ein überwachtes Objekt erhält man sofort Informationen zum Ergebnis der Überwachung.

The screenshot displays the NodeWatch monitoring dashboard. It is organized into three vertical columns representing different locations: Passau, München, and Wien. Each column contains a grid of node cards. Each card shows the node name, its category (e.g., Router, Server, Switch, Firewall), and a status indicator (green for good, yellow for warning, red for error). Some cards also show IP addresses and other details. At the bottom of the dashboard, there is a status bar with various icons and counts, including a user icon, a lock icon, and several numbered icons. The NodeWatch logo and copyright information (© Michael Rothhofer 2016 - 2019) are located in the bottom right corner.

Fordern Sie noch heute eine kostenlose Testversion an!

Web: [www.nodewatch.de](http://www.nodewatch.de)

Mail: [info@nodewatch.de](mailto:info@nodewatch.de)