

Nagios unter UCS

Thema:	Einführung, Installation und Konfiguration von Nagios unter UCS
Datum:	3. April 2011
Seitenzahl:	29
Versionsnummer:	8381
Autoren:	Univention GmbH feedback@univention.de

Inhaltsverzeichnis

1 Einführung	3
1.1 Aufbau von Nagios	4
1.2 Integration in Univention Corporate Server	4
2 Installation	5
2.1 Installation des Nagios-Servers	5
2.2 Installation des Nagios-Clients	5
3 Konfiguration	6
3.1 Domänenweite Konfiguration über den Univention Directory Manager	6
3.2 Konfiguration über Univention Configuration Registry-Variablen	14
3.3 UCS-spezifische Nagios-Plugin-Kommandos	18
3.4 Standard-Nagios-Plugin-Kommandos	20
3.5 Manuelles Einbinden von Nagios-Plugins	26
3.6 Einbindung von manuell erstellten Konfigurationsdateien	27
4 Hinweise / Troubleshooting	28
4.1 NRPE-Fehlermeldung "Could not complete SSL handshake"	28
4.2 Nagios-Konfiguration wird nicht übernommen	28
4.3 Der NRPE Server startet nicht mehr	28
4.4 Nagios-Fehlermeldung "Nagios is currently not checking for external commands"	29

1 Einführung

Mit Hilfe der Software Nagios ist es möglich, komplexe IT-Strukturen aus Netzen, Rechnern und Diensten nachzubilden und deren korrekte Funktion fortlaufend automatisch zu überprüfen. Dazu bringt Nagios eine umfassende Sammlung an Überwachungsmodulen mit. Eine einfache Zustandsabfrage der überwachten Objekte kann durch die mitgelieferte webbasierte Oberfläche getätigt werden, welche die Informationen übersichtlich bereitstellt.

Neben der Abfrage von Kennzahlen (z.B. CPU- und Speicherauslastung, freie Festplattenkapazität) ist Nagios in der Lage, die Funktion unterschiedlicher Dienste (z.B. SSH, SMTP, HTTP) zu testen. Die Tests beschränken sich dabei nicht auf die Erreichbarkeit des Dienstes (z.B. Test des Mailserver-Ports), sondern überprüfen auch die bereitgestellte Funktionalität (z.B. das Ausliefern einer Testmail), um Probleme schnellstmöglich zu identifizieren.

Für die Abfragen bzw. Tests können Grenzwerte festgelegt werden, anhand derer der Zustand eines Dienstes bewertet wird. Beim Überschreiten der Grenzwerte können vorher festgelegte Kontaktpersonen über eine mögliche Fehlfunktion informiert werden.

Neben den in Nagios enthaltenen Plugins zur Durchführung von Tests werden auch Univention-spezifische Plugins mitgeliefert, die die Überwachung von UCS-Kernfunktionalitäten ermöglichen.

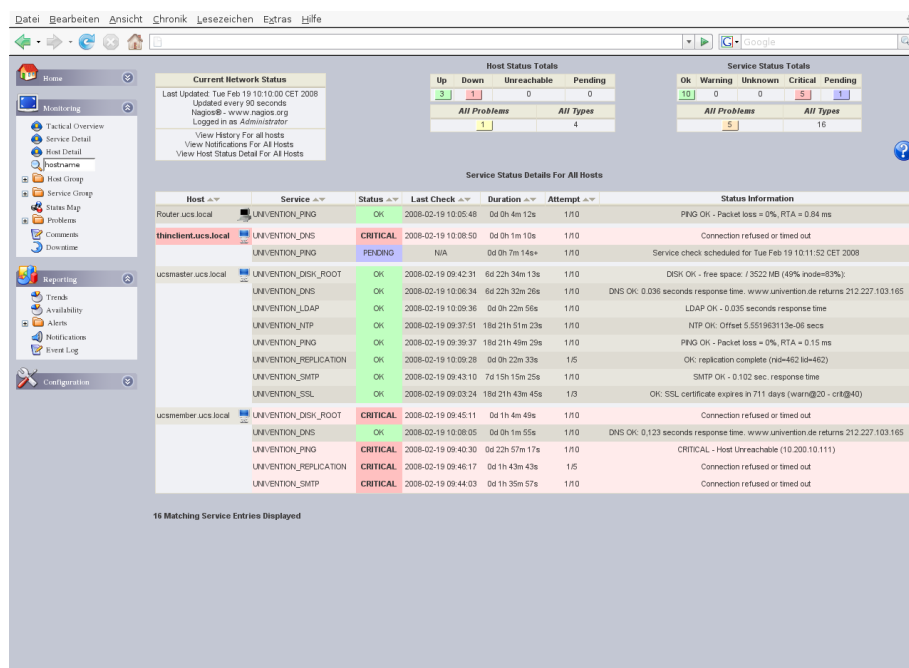


Abbildung 1: Beispiel einer Status-Seite der Nagios-Oberfläche

1.1 Aufbau von Nagios

Nagios unterteilt sich in mehrere Komponenten, die teilweise auf unterschiedlichen Rechnern betrieben werden. Die Kernkomponente von Nagios ist der Nagios-Server (siehe Abbildung 2). Er ist für die Erhebung und Speicherung der Überwachungsdaten zuständig, welche über die webbasierte Nagios-Benutzeroberfläche abgerufen werden können.

Die eigentliche Beschaffung der Überwachungsdaten wird von Nagios-Plugins getätigt, die in regelmäßigen Abständen vom Nagios-Server aufgerufen werden. Sie fragen lokale Kennzahlen ab oder führen Remote-Funktionstests an Diensten durch. Die erhobenen Informationen geben sie anschließend an den Nagios-Server weiter.

Häufig gibt es Situationen, in denen eine Abfrage nicht über das Netz durchgeführt werden kann (z.B. Test des DHCP-Dienstes). In diesem Fall kann der NRPED (Nagios Remote Plugin Executor Daemon) eingesetzt werden, welcher nach einer Anfrage des Nagios-Servers auf dem entfernten Rechner Nagios-Plugins ausführt und die erhobenen Informationen anschließend zurückleitet. Der NRPED und die Nagios-Plugins werden üblicherweise als Nagios-Client zusammengefasst.

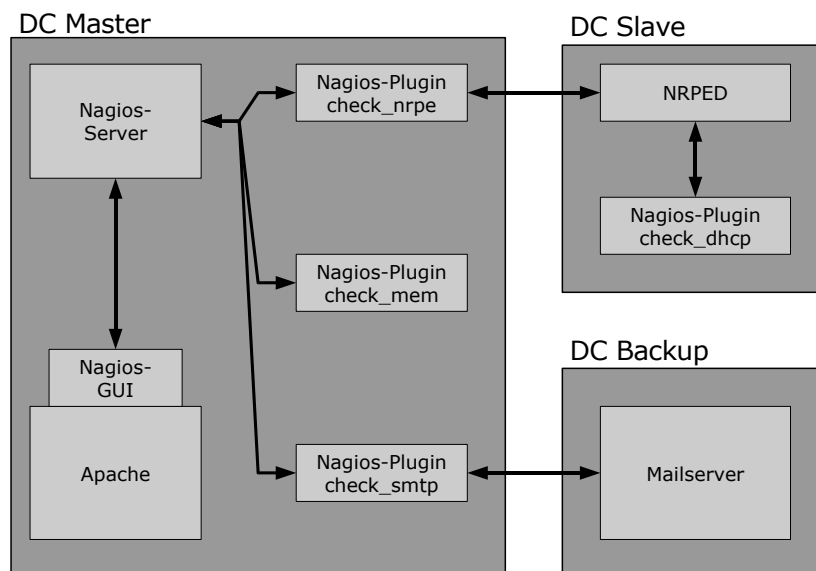


Abbildung 2: Beispielhafte Nagios-Architektur

1.2 Integration in Univention Corporate Server

Durch die Integration in Univention Corporate Server kann die Nagios-Konfiguration komfortabel über den Univention Directory Manager vorgenommen werden. Die von Nagios benötigten Konfigurationsdateien werden automatisch aus den im LDAP-Verzeichnis gespeicherten Informatio-

nen generiert. Dabei bleibt weiterhin die Möglichkeit bestehen, eigene Konfigurationselemente zu der automatisch generierten Konfiguration hinzuzufügen.

2 Installation

Das Nagios-System unterteilt sich in zwei Komponenten: den Nagios-Server und den Nagios-Client. Beide Komponenten können in bestehenden UCS-Umgebungen auf UCS-Domaincontroller-, UCS-Memberserver- und UCS-Managed Client-Systemen installiert werden. Nähere Informationen zur Installation und Aktualisierung von Paketen finden sich auch im Abschnitt “Univention Management Console” des UCS-Handbuchs.

2.1 Installation des Nagios-Servers

Zur Installation des Nagios-Servers auf einem UCS-System muss das Paket **univention-nagios-server** installiert werden. Weitere benötigte Pakete werden als Abhängigkeiten automatisch bei der Installation berücksichtigt.

Nach der erfolgreichen Installation des Pakets kann die Nagios-Oberfläche unter der URL <https://<ip-oder-fqdn>/nagios/> erreicht werden. Die Nagios-Oberfläche ist nur für Benutzer der Gruppe **Domain Admins** und den Benutzer **Administrator** freigegeben. In der Standardeinstellung wird allen anderen Benutzern der Zugriff auf die Nagios-Oberfläche verweigert (siehe dazu auch Abschnitt “Nagios-Oberfläche”).

2.2 Installation des Nagios-Clients

Um einige Dienste auf entfernten UCS-Systemen überprüfen zu können, ist die Installation des Nagios-Clients auf diesen UCS-Systemen notwendig. Die Installation des benötigten Pakets **univention-nagios-client** kann ebenfalls über Univention Management Console initiiert werden. Auch hier werden erforderliche Paketabhängigkeiten, wie der Nagios NRPE Dämon, automatisch mitinstalliert.

Neben der Installation über Univention Management Console ist ebenso eine automatische Verteilung von **univention-nagios-client** auf den UCS-Systemen möglich. Hinweise hierzu finden sich im Abschnitt “Softwareverteilung” des UCS-Handbuchs.

Neben den Standard-Nagios-Plugins, die mit der Installation des Pakets **univention-nagios-client** mitgebracht werden, können zusätzliche Plugins über folgende Pakete nachinstalliert werden:

- **univention-nagios-raid**: Überwachung des Software-RAID-Status
- **univention-nagios-smart**: Prüfung des S.M.A.R.T.-Status von Festplatten
- **univention-nagios-opsi**: Prüfung von OPSI
- **univention-nagios-uvmm**: Überwachung des Univention Virtual Machine Manager

- **univention-nagios-libvirt-d-xen:** Überwachung eines UVMM-Virtualisierungs-Servers auf Basis von Xen
- **univention-nagios-libvirt-d-kvm:** Überwachung eines UVMM-Virtualisierungs-Servers auf Basis von KVM

3 Konfiguration

Bei der Konfiguration des Nagios-Systems wird zwischen domänenweiten und lokalen Einstellungen für UCS-Systeme unterschieden. Die domänenweite Konfiguration des Nagios-Systems wird zentral über den Univention Directory Manager vorgenommen. Hingegen werden lokale Einstellungen für Nagios-Server und Nagios-Client auf den UCS-Systemen über den Univention Configuration Registry-Mechanismus verwaltet. Darüber hinaus ermöglicht das Nagios-System die Einbindung manuell erstellter Konfigurationsdateien.

Hinweis:

Nach der Installation der Nagios-Pakete ist das Nagios-System bereits vorkonfiguriert und betriebsbereit. Es wird automatisch die Überwachung für einige UCS-Dienste eingerichtet, so dass Nagios direkt nach der Installation mit der Überwachung beginnt. Welche Einstellungen automatisch vorgenommen werden, wird nachfolgend in den Abschnitten "Nagios-Zeitraum" und "Nagios-Dienst" erläutert.

3.1 Domänenweite Konfiguration über den Univention Directory Manager

Der Univention Directory Manager bietet Administratoren eine einheitliche Schnittstelle zur Konfiguration des Nagios-Systems. Über spezielle Dialoge kann der Administrator zentral die Konfiguration aller zu überwachender Rechner und Dienste bestimmen sowie die für die Überwachung benötigten Parameter setzen.

Die über den Univention Directory Manager durchgeführten Änderungen im LDAP-Verzeichnis werden automatisch auf die an der Nagios-Überwachung beteiligten UCS-Systeme repliziert und basierend auf diesen Informationen entsprechende Nagios-Konfigurationsdateien erstellt. Ein weiterer Eingriff durch den Administrator ist nicht notwendig.

Die Nagios-Integration in UCS integriert die Univention Directory Manager-Objekte **Nagios:Zeitraum** sowie **Nagios:Dienst**, welche über den Nagios-Assistenten verwaltet werden. Zusätzlich wird der Rechner-Assistent bei der Installation des Pakets **univention-nagios-server** um zwei Nagios-spezifische Karteikarten erweitert.

3.1.1 Nagios-Zeitraum

Nagios:Zeitraum-Objekte werden von **Nagios:Dienst**-Objekten verwendet, um Zeiträume festzulegen, in denen Dienstüberprüfungen stattfinden oder Kontaktpersonen benachrichtigt werden sollen. Die Angabe der Zeiträume wird für jeden einzelnen Wochentag getrennt durchgeführt.

Während der Installation des Nagios-Servers werden drei Standard-Nagios:Zeitraum-Objekte angelegt:

Nagios:Zeitraum	Funktion
24x7	Dieses Objekt definiert einen Zeitraum, der Montags um 0:00 Uhr beginnt und ohne zwischenzeitliche Unterbrechungen am Sonntag um 24:00 Uhr endet.
WorkHours	Definiert die Zeitrahmen von 8 Uhr bis 16 Uhr jeweils von Montag bis Freitag.
NonWorkHours	Ist das Gegenstück zum Nagios:Zeitraum-Objekt WorkHours und deckt die Zeitrahmen von 0 Uhr bis 8 Uhr sowie 16 Uhr bis 24 Uhr jeweils Montag bis Freitag sowie am Samstag und Sonntag jeweils von 0 Uhr bis 24 Uhr ab.

Hinweis:

Die automatisch angelegten Zeitrahmen können manuell verändert oder gelöscht werden. Sie werden jedoch teilweise von den ebenfalls automatisch angelegten Nagios:Dienst-Objekten verwendet. Es ist zu beachten, daß das Löschen eines Nagios:Zeitraum-Objektes nur dann möglich ist, wenn es nicht mehr von Nagios:Dienst-Objekten verwendet wird.

Karteikarte Allgemein
<p>Name Ein eindeutiger Name für das Nagios:Zeitraum-Objekt.</p> <p>Beschreibung Der hier enthaltene Text dient zur Beschreibung des Nagios:Zeitraum-Objektes.</p> <p>Montag Dieses Feld enthält eine Liste von Zeiträumen. Soll für einen Wochentag kein Zeitraum definiert werden, muss das entsprechende Wochentagsfeld leer bleiben. Die Angabe eines Zeitraums erfordert immer zweistellige Stunden- und Minutenangaben, die durch einen Doppelpunkt getrennt werden. Start- und Endzeitpunkt werden durch einen Bindestrich getrennt. Sollen für einen Wochentag mehrere Zeiträume definiert werden, können diese durch ein Komma getrennt in das Textfeld eingetragen werden. Ein ganzer Tag wird durch den Zeitraum 00:00-24:00 repräsentiert.</p> <p>Beispiel: 08:00-12:00,12:45-17:00</p> <p>Dienstag Siehe Montag.</p> <p>Mittwoch Siehe Montag.</p> <p>Donnerstag Siehe Montag.</p>

<p>Freitag Siehe <i>Montag</i>.</p> <p>Samstag Siehe <i>Montag</i>.</p> <p>Sonntag Siehe <i>Montag</i>.</p>
--

3.1.2 Nagios-Dienst

Nagios:Dienst-Objekte definieren die Überwachung eines Dienstes. Einem Nagios:Dienst-Objekt kann eine beliebige Anzahl an Rechnern zugeordnet werden, so dass durch die einmalige Angabe von zu verwendenden Nagios-Plugins sowie Überprüfungs- und Benachrichtigungsparametern eine Dienstüberprüfung auf den angegebenen Rechnern eingerichtet werden kann.

Während der Installation werden automatisch mehrere Nagios:Dienst-Objekte angelegt, um die Kernfunktionen der installierten UCS-Systeme zu überwachen.

Nagios:Dienst	Funktion
UNIVENTION_PING	testet die Erreichbarkeit des überwachten UCS-Systems mit dem Kommando <code>ping</code> . In der Standardeinstellung wird der Fehlerzustand erreicht, wenn die Antwortzeit 50ms bzw. 100ms überschreitet oder Paketverluste von 20% bzw. 40% auftreten.
UNIVENTION_DISK_ROOT	überwacht den Füllstand der <code>/</code> -Partition. Unterschreitet der verbleibende freie Platz in der Standardeinstellung 25% bzw. 10% wird der Fehlerzustand gesetzt.
UNIVENTION_DNS	testet die Funktion des lokalen DNS-Server und die Erreichbarkeit der öffentlichen DNS-Server durch die Abfrage des Rechnernamens <i>www.univention.de</i> . Ist für die UCS-Domäne kein DNS-Forward definiert, schlägt diese Abfrage fehl. In diesem Fall kann <i>www.univention.de</i> z.B. gegen den FQDN des Domaincontroller Master ersetzt werden, um die Funktion des Namensauflösung zu testen.
UNIVENTION_LDAP	überwacht den auf UCS-Domaincontroller-Systemen laufenden LDAP-Server.
UNIVENTION_NTP	fragt auf dem überwachten UCS-System die Uhrzeit beim NTP-Dienst ab. Tritt eine Abweichung von mehr als 60 bzw. 120 Sekunden auf, wird der Fehlerzustand erreicht.
UNIVENTION_SMTP	testet den installierten Mailserver.
UNIVENTION_SSL	testet die verbleibende Gültigkeitsdauer der UCS-SSL-Zertifikate. Dieses Plugin ist nur für Domaincontroller Master- und Domaincontroller Backup-Systeme geeignet.

UNIVENTION_REPLICATION	überwacht den Status der LDAP-Replikation und erkennt das Anlegen einer <code>failed.ldif</code> -Datei sowie den Stillstand der Replikation und warnt vor zu großen Differenzen der Transaktions-IDs.
UNIVENTION_NSCD	testet die Verfügbarkeit des Name Server Cache Dienstes. Läuft kein NSCD-Prozess wird ein CRITICAL-Event ausgelöst, läuft mehr als ein Prozess ein WARNING.
UNIVENTION_WINBIND	testet die Verfügbarkeit des Winbind-Dienstes. Läuft kein Prozess wird ein CRITICAL-Event ausgelöst.
UNIVENTION_SMBD	testet die Verfügbarkeit des Samba-Dienstes. Läuft kein Prozess wird ein CRITICAL-Event ausgelöst.
UNIVENTION_NMBD	testet die Verfügbarkeit des NMBD-Dienstes, der in Samba für den Netbios-Dienst zuständig ist. Läuft kein Prozess wird ein CRITICAL-Event ausgelöst.
UNIVENTION_JOINSTATUS	prüft den Join-Status eines Systems. Ist ein System noch nicht gejoint, wird ein CRITICAL-Event ausgelöst, sind nicht-aufgerufene Join-Skript vorhanden, wird ein WARNING-Event zurückgeliefert.
UNIVENTION_KPASSWD	prüft die Verfügbarkeit des Kerberos-Passwort-Dienstes (nur verfügbar auf Domänencontroller Master/Backup) Läuft weniger oder mehr als ein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_CUPS	überwacht den CUPS-Daemon. Läuft kein cupsd-Prozess oder die Weboberfläche auf Port 631 ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.
UNIVENTION_DANSGUARDIAN	überwacht den Filter Dansguardian. Läuft kein dansguardian-Prozess oder der Dansguardian-Proxy ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.
UNIVENTION_SQUID	überwacht den Proxy Squid. Läuft kein squid-Prozess oder der Squid-Proxy ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.

Für die oben genannten Dienste wurden Standardparameter festgelegt, die auf die Ansprüche der meisten UCS-Installationen zugeschnitten sind. Sollten diese Standardparameter nicht geeignet sein, können sie nachträglich angepasst werden.

Die Nagios-Dienste UNIVENTION_SMART_SDA, UNIVENTION_RAID und UNIVENTION_OPSI sind erst nach der Installation zusätzlicher Pakete auf dem jeweiligen Nagios-Client verfügbar (siehe Abschnitt 2):

Nagios:Dienst	Funktion
UNIVENTION_OPSI	überwacht den OPSI-Daemon. Läuft kein OPSI-Prozess oder die OPSI-Weboberfläche ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.
UNIVENTION_SMART_SDA	prüft den S.M.A.R.T.-Status der Festplatte <code>/dev/sda</code> . Für die Festplatten sdb, sdc und sdd existieren entsprechende Nagios-Dienste.

UNIVENTION_RAID	prüft den Status des Software-RAIDs über <code>/proc/mdadm</code> und gibt CRITICAL, sofern eine Festplatte des RAID-Verbundes ausgefallen, bzw. WARNING zurück, wenn der Recovery-Vorgang läuft.
UNIVENTION_RAID	prüft den Status des Software-RAIDs über <code>/proc/mdadm</code> und gibt CRITICAL, sofern eine Festplatte des RAID-Verbundes ausgefallen, bzw. WARNING zurück, wenn der Recovery-Vorgang läuft.
UNIVENTION_RAID	prüft den Status des Software-RAIDs über <code>/proc/mdadm</code> und gibt CRITICAL, sofern eine Festplatte des RAID-Verbundes ausgefallen, bzw. WARNING zurück, wenn der Recovery-Vorgang läuft.
UNIVENTION_LIBVIRT_KVM	prüft den Status eines KVM-Virtualisierungs-Servers über eine Anfrage an <code>virsh</code> und gibt CRITICAL zurück wenn die Anfrage mehr als zehn Sekunden dauert.
UNIVENTION_LIBVIRT_XEN	prüft den Status eines Xen-Virtualisierungs-Servers über eine Anfrage an <code>virsh</code> und gibt CRITICAL zurück wenn die Anfrage mehr als zehn Sekunden dauert.
UNIVENTION_UVMMD	prüft den Status des Univention Virtual Machine Managers über eine Anfrage der verfügbaren Nodes. Können sie nicht aufgelöst werden, wird CRITICAL zurückgegeben.

Karteikarte Allgemein
<p>Name Ein eindeutiger Name für das Nagios:Dienst-Objekt.</p> <p>Beschreibung Der hier enthaltene Text dient zur Beschreibung des Nagios:Dienst-Objektes.</p> <p>Plugin-Kommando Das Plugin-Kommando identifiziert den Test, der durchgeführt werden soll. Nagios bildet das kurze Plugin-Kommando intern auf eine lange Kommandozeile ab, die bereits passende, vordefinierte Kommandozeilenparameter für das jeweilige Nagios-Plugin enthält. Die verfügbaren Plugin-Kommandos können den Konfigurationsdateien im Verzeichnis <code>/etc/nagios-plugins/config/</code> entnommen werden.</p> <p>Beispiel: check_disk</p> <p>Plugin-Kommando-Parameter Da nicht alle Parameter der Nagios-Plugins in Plugin-Kommandos vordefiniert werden können, ist oft die Angabe zusätzlicher Parameter notwendig. Die hier angegebenen Plugin-Kommando-Parameter werden durch Ausrufungszeichen ("<code>!</code>") getrennt.</p> <p>Beispiel: 20%!10%!/home</p> <p>NRPE benutzen</p>

Kann der Test eines Dienstes nicht remote ausgeführt werden (z.B. der Test eines entfernten DHCP-Servers), kann über den Nagios Remote Plugin Executor Daemon (NRPED) auf einem entfernten UCS-System ein Nagios-Plugin aufgerufen werden. Die dafür notwendige Konfiguration auf dem entfernten UCS-System wird automatisch durchgeführt, sofern das Paket **univention-nagios-client** installiert wurde.

Karteikarte Intervalle

Prüfintervall

Das Prüfintervall definiert den zeitlichen Abstand in Minuten zwischen zwei Überprüfungen des Dienstes.

Beispiel:

10

Prüfintervall im Fehlerfall

Sollte die letzte Überprüfung des Dienstes nicht den Zustand "OK" zurückgeliefert haben, verwendet Nagios ein anderes Zeitintervall für die nächsten Überprüfungen. Im Fehlerfall kann so die Überprüfungsfrequenz erhöht werden. Wurde der Zustand "OK" wieder erreicht, verwendet Nagios wieder das reguläre Prüfintervall. Der Wert ist in der Einheit Minuten anzugeben.

Beispiel:

2

Maximale Anzahl der Überprüfungen

Liefert eine Überprüfung einen Nicht-"OK"-Zustand zurück, wird die hier angegebene Anzahl an Überprüfungen abgewartet, bevor die zuständigen Kontaktpersonen benachrichtigt werden. Erreicht der Dienst vor dem Erreichen des hier angegebenen Limits wieder den Zustand "OK", wird der interne Zähler zurückgesetzt und es findet keine Benachrichtigung statt.

Beispiel:

10

Hinweis:

*Die zeitliche Verzögerung einer Benachrichtigung richtet sich sowohl nach der **maximalen Anzahl an Überprüfungen** als auch dem **Prüfintervall im Fehlerfall**. Bei einem **Prüfintervall im Fehlerfall** von 2 Minuten und einer **maximalen Anzahl an Überprüfungen** von 10 findet die erste Benachrichtigung nach 20 Minuten statt.*

Prüfzeitraum

Um die Überprüfung eines Dienstes zeitlich einzuschränken, kann ein Prüfzeitraum angegeben werden. Außerhalb dieses Zeitraums finden keine Überprüfungen und somit auch keine Benachrichtigungen statt. Dies kann bei Geräten oder Diensten sinnvoll sein, die z.B. über Nacht deaktiviert werden.

Karteikarte Benachrichtigungen

Benachrichtigungsintervall

Ist der Fehlerfall für einen Dienst eingetreten, werden die Kontaktpersonen in dem hier angegebenen Intervall erneut benachrichtigt. Ein Wert von 0 deaktiviert die wiederholte Benachrichtigung. Der Wert ist in der Einheit Minuten anzugeben.

Beispiel:

240

Benachrichtigungszeitraum

Benachrichtigungen an die Kontaktpersonen werden nur in dem hier angegebenen Zeitraum versendet. Wechselt ein Dienst außerhalb des hier angegebenen Zeitraums in einen Nicht-"OK"-Zustand, wird die erste Benachrichtigung erst mit Erreichen des angegebenen Zeitraums versendet, sofern der Nicht-"OK"-Zustand bis dahin erhalten bleibt.

Beispiel:

24x7

Hinweis:

Benachrichtigungen für Störungen, die außerhalb des angegebenen Zeitraums beginnen und enden, werden nicht nachgeholt.

Benachrichtigen, wenn Zustand WARNING erreicht wird

Wechselt der Zustand des Dienstes auf "WARNING", wird eine Benachrichtigung verschickt. Standardeinstellung: **aktiviert**

Benachrichtigen, wenn Zustand CRITICAL erreicht wird

Wechselt der Zustand des Dienstes auf "CRITICAL", wird eine Benachrichtigung verschickt. Standardeinstellung: **aktiviert**

Benachrichtigen, wenn Zustand UNREACHABLE erreicht wird

Wechselt der Zustand des Dienstes auf "UNREACHABLE", wird eine Benachrichtigung verschickt. Standardeinstellung: **aktiviert**

Benachrichtigen, wenn Zustand RECOVERED erreicht wird

Wechselt der Zustand des Dienstes auf "RECOVERED", wird eine Benachrichtigung verschickt. Standardeinstellung: **aktiviert**

Hinweis:

Benachrichtigungen werden beim Erreichen des Zustandes "RECOVERED" nur versendet, wenn zuvor auch eine Benachrichtigung für das ursprüngliche Problem ("WARNING"/"CRITICAL"/"UNREACHABLE") versendet wurde.

Karteikarte Rechner

Zugeordnete Rechner

Die Dienst-Überprüfung wird für bzw. auf den hier zugeordneten Rechnern durchgeführt.

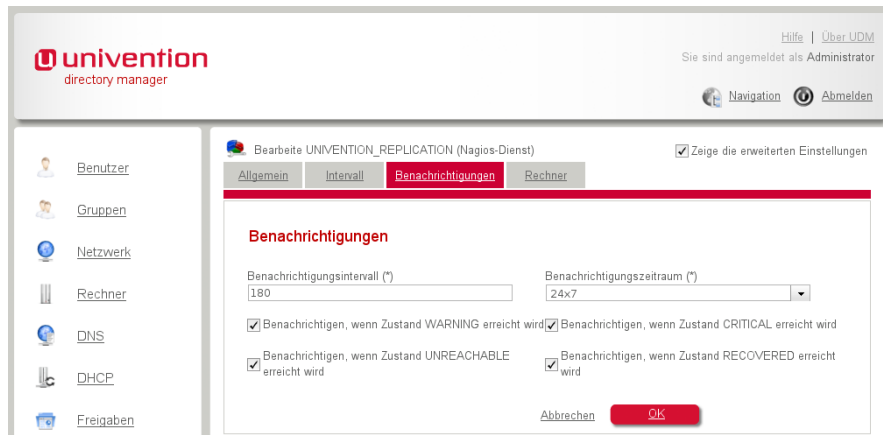


Abbildung 3: Karteikarte "Benachrichtigungen" eines Nagios:Dienst-Objektes

3.1.3 Nagios-spezifische Karteikarten für Rechner-Objekte

Alle in Univention Directory Manager verwaltbaren Rechnerobjekte lassen sich mit Nagios überwachen. Zur Aktivierung der Nagios-Unterstützung muss am betreffenden Rechner-Objekt die Option **Nagios** eingeschaltet werden. Nach der Aktivierung sind zwei zusätzliche Karteikarten am Rechner-Objekt verfügbar, über die u.a. eine komfortable Zuordnung der Nagios-Dienste zum Rechner-Objekt möglich ist.

Karteikarte Nagios-Dienste

Zugeordnete Nagios-Dienste

Es werden hier alle Nagios-Dienste aufgelistet, mit denen das aktuelle Rechner-Objekt verknüpft wurde. Durch das Aufnehmen mehrerer Nagios-Dienste in diese Liste können mehrere Verknüpfungen mit Nagios-Diensten gleichzeitig erstellt werden. Parallel dazu ist weiterhin die Zuordnung von Rechnern am Nagios:Dienst-Objekt möglich.

Nagios-Dienste können nur dann an ein Rechner-Objekt gebunden werden, wenn für diesen eine IP-Adresse sowie ein entsprechender Eintrag für die DNS Forward Zone angegeben wurde.

Karteikarte Nagios-Benachrichtigung

Email-Adressen für Nagios-Benachrichtigungen

Diese Liste enthält die Email-Adressen von Nagios-Kontaktpersonen, die beim Feststellen einer Störung per Email benachrichtigt werden. Werden hier keine Email-Adressen angegeben, wird der lokale Benutzer **root** benachrichtigt.

Übergeordnete Rechner

Durch die Angabe von übergeordneten Rechnern können Abhängigkeiten zwischen Rech-

nen definiert werden. Nagios testet fortlaufend, ob die einzelnen Rechner erreichbar sind. Sollte ein übergeordneter Rechner nicht erreichbar sein, werden keine Benachrichtigungen für Dienststörungen des untergeordneten Rechners versendet. Die angegebenen Abhängigkeiten verwendet Nagios darüber hinaus in der Benutzeroberfläche zur graphischen Darstellung.

Es dürfen keine Schleifen bei der Angabe der übergeordneten Rechner entstehen. Der Nagios-Server wird in diesem Fall die neue Konfiguration nicht übernehmen bzw. sich nicht starten lassen. Hinweise zur Behebung von Schleifen finden sich in Kapitel 4.

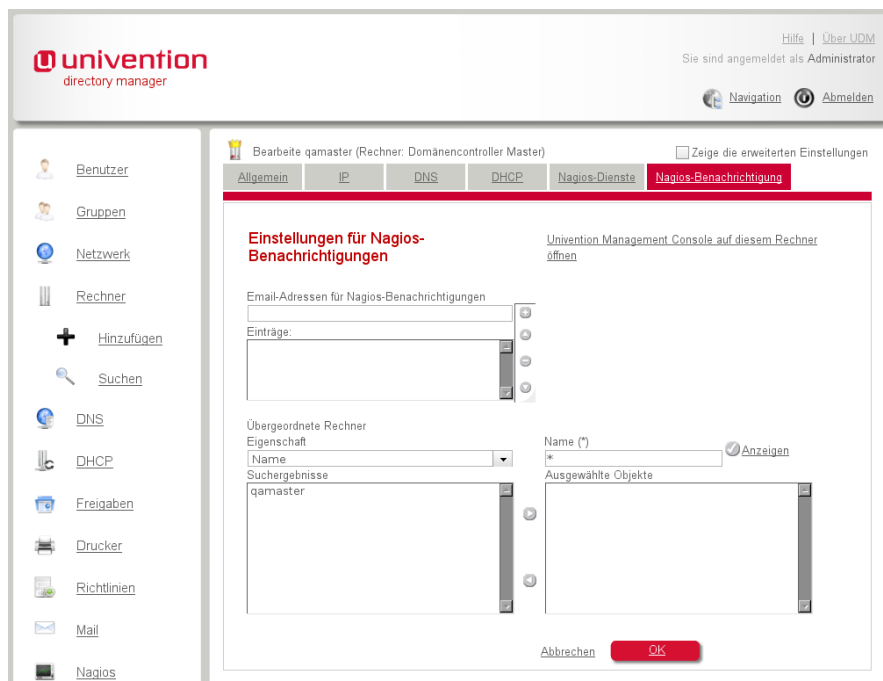


Abbildung 4: Karteikarte "Nagios-Benachrichtigung" eines Domaincontroller Master-Objektes

3.2 Konfiguration über Univention Configuration Registry-Variablen

Lokale Einstellungen am Nagios-System können über die nachfolgend beschriebenen Univention Configuration Registry-Variablen durchgeführt werden. Allgemeine Hinweise zu Univention Configuration Registry finden sich im UCS-Handbuch.

3.2.1 Nagios-Server

Die nachfolgenden Univention Configuration Registry-Variablen verursachen bei einer Veränderung Modifikationen an den Konfigurationsdateien des Nagios-Systems.

Achtung:

Damit diese Modifikationen wirksam werden, ist der Neustart des Nagios-Servers notwendig, welcher über Univention Management Console ausgelöst werden kann.

**nagios/server/autostart**

Werden Änderungen an der Nagios-Konfiguration im LDAP-Verzeichnis vorgenommen, wird der Nagios-Server automatisch neu gestartet. Um den automatischen Neustart zu verhindern, kann die Univention Configuration Registry-Variable auf **no** gesetzt werden. Die Standardeinstellung lautet **yes**.

nagios/server/refreshrate

Die Status-Seiten der Nagios-Benutzeroberfläche aktualisieren sich automatisch in regelmäßigen Abständen. Der Zeitraum zwischen zwei Aktualisierungen kann hier in Sekunden angegeben werden. Die Standardeinstellung beträgt 90 Sekunden.

nagios/server/authenticate

Steht dieser Wert auf **yes**, muss sich der Benutzer gegenüber der Nagios-Benutzeroberfläche authentisieren, um diese nutzen zu können. Steht der Wert auf **no**, kann auch ohne Angabe eines gültigen Benutzerkontos auf die Benutzeroberfläche zugegriffen werden. Die Standardeinstellung lautet **yes**.

nagios/server/user/systeminfo

Der Zugriff auf die Nagios-System- und Prozess-Informationen über die Nagios-Benutzeroberfläche ist auf die hier angegebenen Benutzer beschränkt. Die einzelnen Benutzernamen sind durch Kommata zu trennen. Die Angabe eines Sterns "*" erlaubt allen Benutzern den Zugriff. Die Standardeinstellung lautet *.

Beispiel:

```
nagios/server/user/systeminfo=UserA,User123,UserD
```

nagios/server/user/configinfo

Der Nur-Lese-Zugriff auf die Nagios-Konfiguration über die Nagios-Benutzeroberfläche ist auf die hier angegebenen Benutzer beschränkt. Die einzelnen Benutzernamen sind durch Kommata zu trennen. Die Angabe eines Sterns "*" erlaubt allen Benutzern den Zugriff. Die Standardeinstellung lautet *.

nagios/server/user/systemcmd

Das Veranlassen von Systemkommandos (z.B. das Herunterfahren oder Neustarten des Nagios-Servers) über die Nagios-Benutzeroberfläche ist auf die hier angegebenen Benutzer beschränkt. Die einzelnen Benutzernamen sind durch Kommata zu trennen. Die Angabe eines Sterns "*" erlaubt allen Benutzern den Zugriff. Die Standardeinstellung lautet *.

nagios/server/user/allinfo

Diese Univention Configuration Registry-Variable beschränkt den Benutzerkreis, der in der Lage ist, Informationen über alle Rechner und deren überwachte Dienste über die Nagios-Benutzeroberfläche abzufragen. Die einzelnen Benutzernamen sind durch Kommata zu trennen. Die Angabe eines Sterns "*" erlaubt allen Benutzern den Zugriff. Die Standardeinstellung lautet *.

nagios/server/user/allcmd

Diese Univention Configuration Registry-Variable beschränkt den Benutzerkreis, der in der Lage ist, dienstbezogene Kommandos (z.B. das Aussetzen/Reaktivieren einer Dienstüberwachung) für alle überwachten Dienste über die Nagios-Benutzeroberfläche zu übergeben. Die einzelnen Benutzernamen sind durch Kommata zu trennen. Die Angabe eines Sterns "*" erlaubt allen Benutzern den Zugriff. Die Standardeinstellung lautet *****.

nagios/server/checkexternalcmd

Diese Univention Configuration Registry-Variable ermöglicht es, die Übergabe von Kommandos über Nagios-Benutzeroberfläche generell zu deaktivieren (**no**). Der Wert **yes** ermöglicht die Kommandoübergabe unter Beachtung der oben genannten Univention Configuration Registry-Variablen. Die Standardeinstellung lautet **no**.

nagios/server/hostcheck/enable

Ist diese Univention Configuration Registry-Variable auf **yes** gesetzt, überprüft Nagios regelmäßig die Erreichbarkeit aller eingetragenen Rechner und versendet im Falle der Nichterreichbarkeit eine Nachricht an die eingetragenen Kontaktpersonen. Wird der Wert **no** gesetzt, wird diese Überprüfung deaktiviert. Die Standardeinstellung lautet **yes**.

Hinweis:

*Ist die Erreichbarkeitsüberprüfung deaktiviert, nimmt Nagios für alle Rechner den Zustand **UP** an.*

nagios/server/hostcheck/notificationinterval

Diese Univention Configuration Registry-Variable bestimmt das Wiederbenachrichtigungsintervall für Erreichbarkeitsüberprüfungen von Rechnern. Nach einer Benachrichtigung wird die hier angegebene Anzahl an Minuten gewartet, bevor die nächste Benachrichtigung versendet wird. Die Standardeinstellung lautet **180**.

nagios/server/theme

Diese Univention Configuration Registry-Variable bestimmt das Theme der Nagios-Benutzeroberfläche. Es ist jeweils der Name des gewünschten Themes anzugeben. Ist die Univention Configuration Registry-Variable nicht gesetzt, wird das Standard-Nagios-Theme verwendet. Nach dem Setzen des Themes ist ein Neueinlesen der Apache-Konfigurationsdateien notwendig. Der dafür notwendige Neustart von Apache kann über Univention Management Console vorgenommen werden. In der Standardeinstellung wird das Theme "nuvola" verwendet.

Beispiel:

nagios/server/theme=myCustomTheme

nagios/plugin/check_nrpe/timeout

Diese Univention Configuration Registry-Variable bestimmt die Zeit in Sekunden, die der Nagios-Server auf das Beenden von NRPE-Anfragen wartet. Voreingestellt ist ein Wert von 10 Sekunden.

3.2.2 Nagios-Oberfläche

Der Zugriff zur Nagios-Benutzeroberfläche wird in der Standardeinstellung ausschließlich Benutzern der Gruppe **Domain Admins** gewährt. Über die oben angegebenen Univention Configuration Registry-Variablen kann der Zugriff auf einzelne Funktionen der Oberfläche für diesen Benutzerkreis bzw. einzelne Benutzer weiter eingeschränkt werden. In der Standardeinstellung

– bei den meisten Variablen ist dies * – wird der mögliche Funktionsumfang der Oberfläche nicht weiter eingegrenzt.

Durch die Aufnahme des Dienstes **nagios** in die Univention Configuration Registry-Variable `auth/user/services` kann auch Benutzern ohne Administrator-Rechte der Zugriff auf die Nagios-Oberfläche gewährt werden.

Um den Zugriff zur Nagios-Oberfläche für selbstdefinierte Gruppen freizugeben, kann eine eigene Datei zur Zugriffssteuerung erstellt werden. Als Vorlage kann hier die Datei `/etc/security/access-admin.conf` verwendet werden. Der vollständige Pfad zur der selbstgestellten Datei muss anschließend in die Univention Configuration Registry-Variable `auth/nagios/accessfile` eingetragen werden. Diese Angabe funktioniert nur in Verbindung mit der Aufnahme von **nagios** in die Univention Configuration Registry-Variable `auth/user/services` (siehe oben).

Das optionale Paket **univention-nagios-group-access** führt diese Schritte bei seiner Installation automatisch durch. Es erstellt über ein Joinskript die Benutzergruppe **Nagios Admins**, die in der Standardeinstellung neben der Gruppe **Domain Admins** Zugriff auf die Nagios-Oberfläche erhält. Davon abweichend kann über die Univention Configuration Registry-Variable `nagios/server/webaccess/groups` eine kommaseparierte Liste an Benutzergruppen angegeben werden, die Zugriff auf die Nagios-Oberfläche erhalten sollen. Das Paket ist auf dem Nagios-Server zu installieren.

3.2.3 Nagios-Client

Die nachfolgenden Univention Configuration Registry-Variablen verursachen bei einer Veränderung Modifikationen an den Konfigurationsdateien des Nagios-Systems. Der Dienst **Nagios NRPE Server** muss anschließend über Univention Management Console neu gestartet werden, damit diese Änderungen wirksam werden.

nagios/client/autostart

Werden Änderungen an der Nagios-Konfiguration im LDAP-Verzeichnis vorgenommen, wird der Nagios-NRPE-Server automatisch neu gestartet. Um den automatischen Neustart zu verhindern, kann die Univention Configuration Registry-Variable auf **no** gesetzt werden. Die Standardeinstellung lautet **yes**.

nagios/client/allowedhosts

Diese Univention Configuration Registry-Variable beschränkt den Kreis der Rechner, die auf den gestarteten NRPE-Dienst zugreifen dürfen. Die Angabe der erlaubten Rechner erfolgt über ihren FQDN oder ihre IP-Adresse. Ist diese Univention Configuration Registry-Variable nicht gesetzt, wird automatisch der FQDN des UCS-Domaincontroller Master eingetragen. In der Standardeinstellung ist diese Univention Configuration Registry-Variable nicht gesetzt.

Beispiel:

`nagios/client/allowedhosts=127.0.0.1,someserver.somedomain.intra,10.200.18.30`

nagios/client/checkraid

Um eine regelmäßige Überprüfung des Zustandes des lokalen Festplatten-RAID-Systems durchzuführen, muss diese Univention Configuration Registry-Variable auf **yes** gesetzt werden. Ein Wert von **no** deaktiviert die Überprüfung. Die Standardeinstellung lautet **no**.

nagios/client/autoregister

Während der Installation von **univention-nagios-client** bzw. beim manuellen Ausführen des im Paket enthaltenen Join-Skripts wird für den Client die Überwachung für Standard-Dienste eingerichtet. Um die Einrichtung zu unterbinden, kann vor der Installation des Pakets die Univention Configuration Registry-Variable auf **no** gesetzt werden. In der Standardeinstellung ist diese Univention Configuration Registry-Variable nicht gesetzt.

3.3 UCS-spezifische Nagios-Plugin-Kommandos

Mit den Nagios-Paketen werden auch UCS-spezifische Nagios-Plugins mitgeliefert, welche spezielle Funktionen des UCS-System überwachen können.

- `check_univention_printerqueue`
Das Nagios-Plugin-Kommando wurde für die Überwachung von Druckerqueues entwickelt und erwartet die Plugin-Kommando-Parameter **warncnt!critcnt!queue**.

Parameter	Funktion
warncnt	(Ganzzahl) Erreicht die Anzahl der Druckjobs in der Druckerqueue diesen Wert, wechselt der Zustand auf "WARNING".
critcnt	(Ganzzahl) Erreicht die Anzahl der Druckjobs in der Druckerqueue diesen Wert, wechselt der Zustand auf "CRITICAL".
queue	(Zeichenkette) Name der zu überwachenden Druckerqueue.

Beispiel:

10!20!Laserdrucker

- `check_univention_printerqueue_disabled`
Das Nagios-Plugin-Kommando wurde für die Überwachung von Druckerqueues entwickelt und erwartet die gleichen Plugin-Kommando-Parameter wie `check_univention_printerqueue`. Zusätzlich liefert es den Zustand "WARNING" zurück, wenn die Druckerqueue deaktiviert wurde.
- `check_univention_i2oraid_physical`
`check_univention_i2oraid_logical`
`check_univention_i2oraid_raid`
`check_univention_i2oraid_controller`
Die vier Nagios-Plugin-Kommandos ermöglicht die Überwachung eines I2O-RAID-Controllers. Sie testen:
 - den Status der am RAID beteiligten Festplatten ("physical"),
 - die Integrität des RAIDs ("logical"),
 - den Status des RAIDs und der beteiligten Festplatten ("raid"),
 - den Status des RAID-Controllers ("controller").

Die Plugin-Kommandos erwarten den Kommando-Parameter **device**.

Parameter	Funktion
device	(Ganzzahl) Nummer das RAID-Devices.

- `check_univention_replication`
Das Nagios-Plugin-Kommando überprüft die LDAP-Replikation und ermittelt Transaktions-ID des UCS-Domaincontroller Master sowie die Transaktions-ID des zu testenden Systems. Sollte die Differenz zwischen den beiden Transaktions-IDs zu groß werden bzw. sich die Transaktions-ID des zu testenden UCS-Systems über längere Zeit nicht verändern, wird auf einen entsprechenden Fehlerzustand gewechselt. Das Nagios-Plugin-Kommando erwartet die Plugin-Kommando-Parameter ***cnt!warndiff!critdiff***.

Parameter	Funktion
<i>cnt</i>	(Ganzzahl) Sind die Transaktions-IDs ungleich und es fand auf dem zu testenden UCS-System für <i>cnt</i> Überprüfungen keine Änderung der Transaktions-ID statt, wechselt der Zustand auf "CRITICAL".
<i>warndiff</i>	(Ganzzahl) Erreicht die Differenz zwischen den beiden oben genannten Transaktions-IDs den Wert <i>warndiff</i> , wechselt der Zustand auf "WARNING".
<i>critdiff</i>	(Ganzzahl) Erreicht die Differenz zwischen den beiden oben genannten Transaktions-IDs den Wert <i>critdiff</i> , wechselt der Zustand auf "CRITICAL".

Beispiel:
10!50!100

- `check_univention_nfsstatus`
Das Nagios-Plugin-Kommando testet den Mount-Status der in der Datei `/etc/fstab` eingetragenen NFS-Freigaben. Sind nicht alle mit der Option "auto" gekennzeichneten NFS-Freigaben gemountet, wechselt der Zustand auf "CRITICAL".
- `check_univention_nfsstatus_all`
Das Nagios-Plugin-Kommando testet den Mount-Status der in der Datei `/etc/fstab` eingetragenen NFS-Freigaben. Sind nicht alle NFS-Freigaben gemountet, wechselt der Zustand auf "CRITICAL".
Achtung:
Dieses Plugin-Kommando testet auch NFS-Freigaben, die mit der Option "noauto" in der Datei `/etc/fstab` eingetragen wurden!
- `check_univention_sslcert`
Das Nagios-Plugin-Kommando warnt vor dem Ablauf des lokalen SSL-Zertifikats. Es erwartet den Plugin-Kommando-Parameter ***warndays!critdays***. Dieses Plugin-Kommando kann nur auf UCS-Systemen mit der Systemrolle Domaincontroller Master oder Domaincontroller Backup eingesetzt werden.

Parameter	Funktion
<i>warndays</i>	(Ganzzahl) Ist das SSL-Zertifikat <i>warndays</i> oder weniger Tage gültig, wechselt der Zustand auf "WARNING".
<i>critdays</i>	(Ganzzahl) Ist das SSL-Zertifikat <i>critdays</i> oder weniger Tage gültig, wechselt der Zustand auf "CRITICAL".



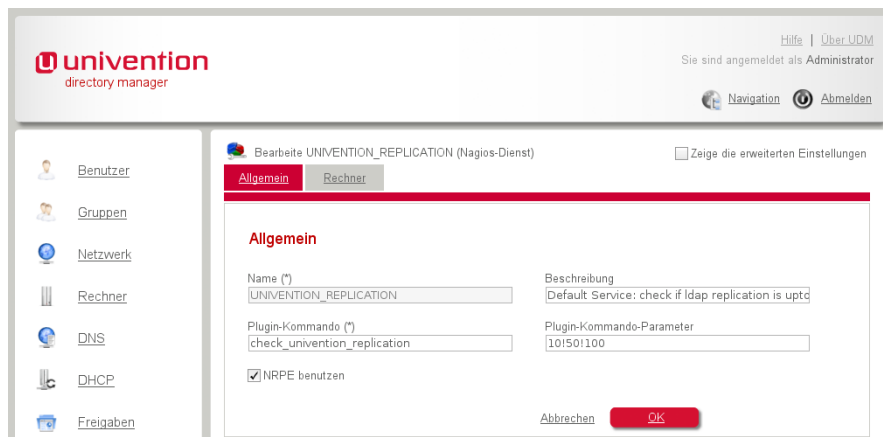


Abbildung 5: Beispielhafte Verwendung des `check_univention_replication`-Kommandos

3.4 Standard-Nagios-Plugin-Kommandos

Nachfolgend werden einige ausgewählte Nagios-Plugin-Kommandos beschrieben, die in der Standard-Installation bereits vorhanden sind. Sie bieten eine gute Übersicht über die bereits installierten Plugins. Dabei muss beachtet werden, dass die aufgelisteten Nagios-Plugin-Kommandos nur einen geringen Teil der Funktionalitäten der Nagios-Plugins abdecken.

Durch eine manuelle Erweiterung der Nagios-Plugin-Konfiguration kann mit zusätzlichen Parametern speziell auf die lokalen Gegebenheiten eingegangen werden, wodurch sich Dienste können präziser und mit geringerer Anzahl an Fehlalarmen überwachen lassen.

- `check_dhcp`
Das Nagios-Plugin-Kommando versucht aktiv ein DHCP-Lease anzufordern. Voraussetzung ist, dass sich der DHCP-Server im lokalen Netz befindet oder der Test über NRPE auf dem DHCP-Server durchgeführt wird. Dieses Plugin-Kommando benötigt keine Plugin-Kommando-Parameter.
- `check_dhcp_interface`
Das Nagios-Plugin-Kommando versucht ein DHCP-Lease von den mit diesem Nagios-Dienst verknüpften Rechnern anzufordern. Voraussetzung ist, dass sich der DHCP-Server im lokalen Netz befindet oder der Test über NRPE auf dem DHCP-Server durchgeführt wird. Das Nagios-Plugin-Kommando erwartet den Plugin-Kommando-Parameter ***interface***.

Parameter	Funktion
<i>interface</i>	(Zeichenkette) Name des Netzwerk-Interfaces (z.B. eth0) über das ein DHCP-Lease angefordert wird.

- `check_disk`
Das Nagios-Plugin-Kommando prüft den freien Speicherplatz auf der angegebenen lokalen Partition. Dieses Plugin-Kommando kann nur auf dem Nagios-Server selbst oder über NRPE auf dem Zielsystem ausgeführt werden. Es werden folgende Plugin-Kommando-Parameter erwartet: ***warn!crit!partition***.

Parameter	Funktion
<i>warn</i>	(Ganzzahl oder Prozent) Zustand WARNING, wenn weniger als die hier angegebene Menge an freiem Speicherplatz verfügbar ist. Die Angabe kann als Ganzzahl in MB oder als prozentuale Angabe erfolgen (siehe Beispiel).
<i>crit</i>	(Ganzzahl oder Prozent) Zustand CRITICAL, wenn weniger als die hier angegebene Menge an freiem Speicherplatz verfügbar ist. Die Angabe kann als Ganzzahl in MB oder als prozentuale Angabe erfolgen (siehe Beispiel).

Es kann nur auf dem Nagios-Server selbst oder über NRPE auf dem Zielsystem ausgeführt werden. Es werden folgende Plugin-Kommando-Parameter erwartet: **warn!crit**.

Parameter	Funktion
warn	(Ganzzahl oder Prozent) Zustand WARNING, wenn weniger als die hier angegebene Menge an freiem Speicherplatz verfügbar ist. Die Angabe kann als Ganzzahl in MB oder als prozentuale Angabe erfolgen (siehe Beispiel).
crit	(Ganzzahl oder Prozent) Zustand CRITICAL, wenn weniger als die hier angegebene Menge an freiem Speicherplatz verfügbar ist. Die Angabe kann als Ganzzahl in MB oder als prozentuale Angabe erfolgen (siehe Beispiel).

Beispiel:

1500!5%

- `check_disk_smb_workgroup_host_user`
Das Nagios-Plugin-Kommando prüft den freien Speicherplatz auf einer Samba- bzw. Windows-Freigabe. Es erwartet die Plugin-Kommando-Parameter **netbiosname!share!workgroup!username!password**.

Parameter	Funktion
netbiosname	(Zeichenkette) NetBIOS-Name des Rechner, der die Freigabe share bereitstellt.
share	(Zeichenkette) Name der zu testenden Freigabe.
workgroup	(Zeichenkette) Name der Arbeitsgruppe oder Domäne, in der sich der Rechner netbiosname befindet.
username	(Zeichenkette) Benutzername, der für die Anmeldung an der Freigabe verwendet wird.
password	(Zeichenkette) Passwort, das für die Anmeldung an der Freigabe verwendet wird (Achtung: das Passwort steht im Klartext im LDAP-Verzeichnis! Ggf. Gast-Benutzer mit eingeschränkten Rechten verwenden!).

Beispiel:

WINSRV001!DOKUMENTE!Workgroup!testuser!geheim

Es existieren weitere Plugin-Kommandos, die sich nur in der Anzahl ihrer Plugin-Kommando-Parameter unterscheiden:

Plugin-Kommando	Erwartete Plugin-Kommando-Parameter
<code>check_disk_smb</code>	netbiosname!share
<code>check_disk_smb_workgroup</code>	netbiosname!share!workgroup
<code>check_disk_smb_host</code>	netbiosname!share
<code>check_disk_smb_workgroup_host</code>	netbiosname!share!workgroup
<code>check_disk_smb_user</code>	netbiosname!share!username! password
<code>check_disk_smb_workgroup_user</code>	netbiosname!share!workgroup! username!password

check_disk_smb_host_user	netbiosname!share!username! passwort
--------------------------	---

- `check_dig`
Das Nagios-Plugin-Kommando prüft die Funktionalität eines DNS-Servers und macht eine DNS-Abfrage für den angegebenen FQDN. Erwartete Plugin-Kommando-Parameter: **fqdn**.

Parameter	Funktion
fqdn	(Zeichenkette) Es wird die DNS-Abfrage für den angegebenen FQDN getestet.

- `check_ftp`
Das Nagios-Plugin-Kommando prüft den Verbindungsaufbau zu einem FTP-Server. Plugin-Kommando-Parameter werden nicht benötigt.
- `check_hpjd`
Das Nagios-Plugin-Kommando liest den Status von HP Druckern mit JetDirect-Karte über eine SNMP-Abfrage aus. Es wird automatisch **public** als SNMP Community Name verwendet. Plugin-Kommando-Parameter werden nicht benötigt.
- `check_http`
`check_https`
Diese Nagios-Plugin-Kommandos testen den Abruf einer Seite/Datei von einem HTTP/HTTPS-Server. Dabei wird der FQDN der im Univention Directory Manager verknüpften Rechner für die HTTP/HTTPS-Abfrage verwendet.
- `check_http2`
Das Nagios-Plugin-Kommando testet den Abruf einer Seite/Datei von einem HTTP-Server unter Verwendung des angegebenen Hostnamen. Das Plugin-Kommando kann als Funktionstest für Virtual Hosts verwendet werden und erwartet die Plugin-Kommando-Parameter **hostname!warn!crit**.

Parameter	Funktion
hostname	(Zeichenkette) Hostname, der für die HTTP-Abfrage verwendet wird (Virtual Hosts).
warn	(Ganzzahl) Maximale Abfragedauer in Sekunden, bevor Zustand WARNING erreicht wird.
crit	(Ganzzahl) Maximale Abfragedauer in Sekunden, bevor Zustand CRITICAL erreicht wird.

Beispiel:

virtualhost.domain.de!3!6

- `check_squid`
Das Nagios-Plugin-Kommando testet einen HTTP-Server oder HTTP-Proxy auf einem Nicht-Standard-Port. Plugin-Kommando-Parameter: **port!URL**

Parameter	Funktion
port	(Ganzzahl) Port-Nummer des HTTP-Servers

url	(Zeichenkette) URL, die abfragt wird.
------------	---------------------------------------

Beispiel:

3128!/index.html

- `check_https_auth`
Das Nagios-Plugin-Kommando testet den Abruf einer Seite/Datei von einem HTTPS-Server. Dabei werden Rechner-FQDN sowie die angegebenen Anmeldeinformationen für die HTTPS-Abfrage verwendet. Plugin-Kommando-Parameter: **credentials**

Parameter	Funktion
credentials	(Zeichenkette) Anmeldeinformationen im Format benutzer:passwort

Beispiel:

mmustermann!g3he1m

- `check_ldap`
Das Nagios-Plugin-Kommando prüft einen LDAP-Server und erwartet den Plugin-Kommando-Parameter **basedn**.

Parameter	Funktion
basedn	(Zeichenkette) BasisDN des zu testenden LDAP-Servers.

- `check_pop`
`check_spop`
Diese Nagios-Plugin-Kommandos verbinden sich mit einem POP3-Server unverschlüsselt auf Port 110 bzw. über eine SSL-Verbindung auf Port 995. Plugin-Kommando-Parameter werden nicht benötigt.
- `check_imap`
`check_simap`
Diese Nagios-Plugin-Kommandos verbinden sich mit einem IMAP-Server unverschlüsselt auf Port 143 bzw. über eine SSL-Verbindung auf Port 993. Plugin-Kommando-Parameter werden nicht benötigt.
- `check_smtp`
`check_ssmtp`
Diese Nagios-Plugin-Kommandos verbinden sich mit einem SMTP-Server unverschlüsselt auf Port 25 bzw. über eine SSL-Verbindung auf Port 465. Plugin-Kommando-Parameter werden nicht benötigt.
- `check_mysql`
Das Nagios-Plugin-Kommando verbindet sich mit einer mySQL-Datenbank auf Port 3306 und testet den Verbindungsaufbau. Plugin-Kommando-Parameter werden nicht benötigt.
- `check_mysql_cmdlinecred`
Das Nagios-Plugin-Kommando verbindet sich mit einer mySQL-Datenbank auf Port 3306 und testet den Verbindungsaufbau. Für die Anmeldung werden die Anmeldeinformationen aus den Plugin-Kommando-Parametern **username!password** verwendet.

Parameter	Funktion
-----------	----------

username	(Zeichenkette) Benutzername für die Anmeldung an der MySQL-Datenbank.
password	(Zeichenkette) Passwort für die Anmeldung an der MySQL-Datenbank.

- `check_ntp`
Das Nagios-Plugin-Kommando macht eine NTP-Zeitabfrage bei den im Univention Directory Manager verknüpften NTP-Servern. Plugin-Kommando-Parameter werden nicht benötigt.
- `check_ntp_ntpq`
Das Nagios-Plugin-Kommando macht eine NTP-Zeitabfrage bei den im Univention Directory Manager verknüpften NTP-Servern und prüft den Jitter zu anderen NTP-Servern. Liegt dieser oberhalb von 10 bzw. 15ms wird der Zustand WARNING bzw. CRITICAL erreicht. Plugin-Kommando-Parameter werden nicht benötigt.
- `check_pgsql`
Das Nagios-Plugin-Kommando baut eine unverschlüsselte Verbindung zu einer PostgreSQL-Datenbank auf. Wird diese Verbindung abgelehnt oder die Datenbank ist nicht erreichbar, wechselt der Zustand auf CRITICAL.
- `check_ping`
Das Nagios-Plugin-Kommando testet die Erreichbarkeit von Rechnern und misst dabei die Umlaufzeiten der Pakete. Es werden die Plugin-Kommando-Parameter **warn!crit** erwartet.

Parameter	Funktion
warn	(Zeichenkette) Schwellwert, ab dem der Zustand auf WARNING wechselt. Es muss dabei die maximale Umlaufzeit in ms sowie der maximale Paketverlust in Prozent angegeben werden (siehe Beispiel).
crit	(Zeichenkette) Schwellwert, ab dem der Zustand auf CRITICAL wechselt. Es muss dabei die maximale Umlaufzeit in ms sowie der maximale Paketverlust in Prozent angegeben werden (siehe Beispiel).

Beispiel:

500,100%!1000,80%

- `snmp_load`
Das Nagios-Plugin-Kommando liest via SNMP die OIDs **.1.3.6.1.4.1.2021.10.1.5.1**, **.1.3.6.1.4.1.2021.10.1.5.2** und **.1.3.6.1.4.1.2021.10.1.5.3** aus und gibt die Last auf dem betreffenden System zurück. Es erwartet die Plugin-Kommando-Parameter **warn1!warn5!warn15!crit1!crit5!crit15**.

Parameter	Funktion
warn1	(Ganzzahl) Maximale Last über 1 min, bevor der Zustand auf WARNING wechselt.
warn5	(Ganzzahl) Maximale Last über 5 min, bevor der Zustand auf WARNING wechselt.

warn15	(Ganzzahl) Maximale Last über 15 min, bevor der Zustand auf WARNING wechselt.
crit1	(Ganzzahl) Maximale Last über 1 min, bevor der Zustand auf CRITICAL wechselt.
crit5	(Ganzzahl) Maximale Last über 5 min, bevor der Zustand auf CRITICAL wechselt.
crit15	(Ganzzahl) Maximale Last über 15 min, bevor der Zustand auf CRITICAL wechselt.

- `snmp_disk2`

Das Nagios-Plugin-Kommando liest via SNMP die MIB ***host.hrStorage.hrStorageTable.hrStorageEntry.hrStorageUsed.NUMBER*** aus und gibt den belegten Platz auf dem entsprechenden Speichermedium aus. Das Speichermedium wird dabei über NUMBER identifiziert. Das Plugin-Kommando erwartet die Plugin-Kommando-Parameter ***community!NUMBER!warn!crit***.

Parameter	Funktion
community	(Zeichenkette) SNMP Community Name
NUMBER	(Ganzzahl) Id des Speichermediums (von Betriebssystem und Hardwarekonfiguration abhängig)
warn	(Zeichenkette) Wertebereich, der nicht im Zustand WARNING resultieren soll. Der Wertebereich ist dabei als unterer und oberer Schwellwert anzugeben, welche durch einen Doppelpunkt getrennt werden. Die Einheit des per SNMP ausgelesenen Wertes ist abhängig vom Betriebssystem und wird z.B. in 4 kByte-Blöcken angegeben.
crit	(Zeichenkette) Wertebereich, der nicht im Zustand CRITICAL resultieren soll. Der Wertebereich ist dabei als unterer und oberer Schwellwert anzugeben, welche durch einen Doppelpunkt getrennt werden. Die Einheit des per SNMP ausgelesenen Wertes ist abhängig vom Betriebssystem und wird z.B. in 4 kByte-Blöcken angegeben.

Beispiel:

`public!2!0:25000!0:28000`

- `snmp_procs`

Das Nagios-Plugin-Kommando liest via SNMP die MIB ***host.hrSystem.hrSystemProcesses*** aus und gibt die Anzahl der laufenden Systemprozesse zurück. Es erwartet die Plugin-Kommando-Parameter ***community!warn!crit***.

Parameter	Funktion
community	(Zeichenkette) SNMP Community Name
warn	(Ganzzahl) Maximale Anzahl der Prozesse, bevor der Zustand auf WARNING wechselt.
crit	(Ganzzahl) Maximale Anzahl der Prozesse, bevor der Zustand auf CRITICAL wechselt.

- `snmp_users`
Das Nagios-Plugin-Kommando liest via SNMP die MIB `host.hrSystem.hrSystemNumUsers` aus und gibt die Anzahl der eingeloggten Benutzer zurück. Es erwartet die Plugin-Kommando-Parameter **`community!warn!crit`**.

Parameter	Funktion
<code>community</code>	(Zeichenkette) SNMP Community Name
<code>warn</code>	(Ganzzahl) Maximale Anzahl der Benutzer, bevor der Zustand auf WARNING wechselt.
<code>crit</code>	(Ganzzahl) Maximale Anzahl der Benutzer, bevor der Zustand auf CRITICAL wechselt.

- `check_tcp`
Das Nagios-Plugin-Kommando testet, ob der angegebene TCP-Port geöffnet ist. Dabei wird kein Funktionstest der betreffenden Anwendung durchgeführt! Es erwartet den Plugin-Kommando-Parameter **`port`**.

Parameter	Funktion
<code>port</code>	(Ganzzahl) TCP-Port, der getestet werden soll.

3.5 Manuelles Einbinden von Nagios-Plugins

Nagios zeichnet sich unter anderem durch die Erweiterbarkeit mit zusätzlichen Plugins aus. Im Internet wird eine Vielzahl neuer Plugins für teilweise sehr spezielle Überwachungsaufgaben angeboten. Die folgende Anleitung erläutert, wie das in UCS integrierte Nagios um zusätzliche Plugins erweitert werden kann.

Schritte für das manuelle Einspielen eines zusätzlichen Nagios-Plugins auf einem UCS-System:

- Für manuell eingespielte Nagios-Plugins sollte ein separates Verzeichnis angelegt werden, um zu verhindern, dass Dateien durch nachträglich installierte Pakete überschrieben werden. Sollte das Verzeichnis schon existieren, kann dieser Punkt übersprungen werden.

```
mkdir -p /usr/lib/nagios/plugins.local/
```

- Das ausführbare Nagios-Plugin ist dann im Verzeichnis `/usr/lib/nagios/plugins.local/` abzulegen.
- Gegebenenfalls werden für das Nagios-Plugin zusätzliche Bibliotheken bzw. Pakete benötigt. Diese sind ebenfalls an geeigneter Stelle zu installieren.
- Für die Verwendung des Plugins in Nagios wird eine sogenannte Makro-Datei (z.B. `local.cfg`) im Verzeichnis `/etc/nagios-plugins/config/` benötigt. Sie enthält eine oder mehrere Abbildungen von einem Nagios-Plugin-Kommando auf eine Befehlszeile inklusive benötigter Parameter.

Das folgende Beispiel definiert das Nagios-Plugin-Kommando **`check_local1`** mit drei Platzhaltern (**`$ARG1$`**, **`$ARG2$`** und **`$ARG3$`**) und führt das Plugin **`check_new_plugin`** aus.

Die einzelnen Parameter sind abhängig vom jeweiligen Plugin. Die meisten Plugins liefern eine Beschreibung aller möglichen Parameter, wenn sie mit dem Parameter **-h** aufgerufen werden.

Beispiel:

```
/usr/lib/nagios/plugins.local/check_new_plugin -h
```

```
define command{
  command_name    check_local1
  command_line    /usr/lib/nagios/plugins.local/check_new_plugin
                  -w $ARG1$ -c $ARG2$ $ARG3$
}
```

(Aus Gründen der Lesbarkeit wurde die Zeile **command_line** umgebrochen. Sie ist in der Makro-Datei als eine Zeile ohne Zeilenumbruch anzugeben!)

- Abschließend ist der Nagios-Daemon auf dem UCS-System neuzustarten. Dies kann über den Befehl `/etc/init.d/nagios2 restart` erreicht werden.

Die Installation des Plugins ist damit abgeschlossen. Anschließend kann im Univention Directory Manager ein neues Nagios-Dienst-Objekt im Nagios-Assistenten angelegt werden, bei dem unter **Nagios-Plugin-Kommando** das neue Makro **check_local1** eingetragen werden kann. Im Eingabefeld **Plugin-Kommando-Parameter** können Werte für die einzelnen Platzhalter (für das obige Beispiel **\$ARG1\$**, **\$ARG2\$** und **\$ARG3\$**) eingetragen werden. Die Werte sind durch Ausrufungszeichen zu trennen:

Beispiel:

```
30%!50%!/var/spool/mail
```

Sofern der NRPE (Nagios Remote Plugin Executor) nicht verwendet wird, reicht es aus, die oben genannten Schritte auf dem Nagios-Server durchzuführen. Dies ist bei Plugins der Fall, die sich Informationen ausschließlich über Anfragen über das lokale Netz verschaffen.

Kommt der NRPE zum Einsatz, muss das neue Nagios-Plugin auch auf anderen UCS-Systemen installiert werden, da der NRPE-Daemon Plugins auf dem entfernten System ausführt, um dort Informationen zu sammeln (z.B. um lokal den Zustand des RAID-Controllers auslesen).

Sollen zusätzliche Plugins auf mehreren UCS-Systemen eingespielt werden, kann der Aufwand für die Verteilung durch die Paketierung des Plugins (inklusive Makro-Datei) erheblich verringert werden. Für die Erstellung von Debian-Paketen für und mit UCS stellen wir ein separates technisches Dokument bereit.

3.6 Einbindung von manuell erstellten Konfigurationsdateien

Sollen zu den automatisch erstellten Nagios-Server-Konfigurationsdateien manuell Erweiterungen hinzugefügt werden, können die manuell erstellten Konfigurationsdateien im Verzeichnis `/etc/nagios2/conf.local.d/` abgelegt werden. Nach dem Neustart des Nagios-Servers z.B. über Univention Management Console werden die hinzugefügten Konfigurationsdateien beachtet.

Erweiterungen der NRPE-Konfiguration können im Verzeichnis `/etc/nagios/nrpe.local.d/` abgelegt werden. Die Erweiterungen werden mit dem

Neueinlesen der NRPE-Konfiguration aktiviert. Der dafür notwendige Neustart des **Nagios NRPE Daemons** kann über Univention Management Console durchgeführt werden.

4 Hinweise / Troubleshooting

Wird die Konfiguration von Nagios manuell erweitert, kann es zu Inkonsistenzen in der Nagios-Konfiguration kommen. Die folgenden Hinweise sollen helfen, Probleme mit Nagios schneller zu lokalisieren und zu beheben.

4.1 NRPE-Fehlermeldung “Could not complete SSL handshake”

Die Fehlermeldung **Could not complete SSL handshake** wird zurückgegeben, wenn der Nagios-Server den NRPE des Nagios-Client erreichen konnte und es anschließend Probleme während der Aushandlung der Verschlüsselungsparameter gegeben hat. Dies ist meistens der Fall, wenn auf dem Nagios-Client die Univention Configuration Registry-Variablen `nagios/client/allowedhosts` nicht korrekt gesetzt wurde und der Nagios-Server dadurch abgelehnt wird.

4.2 Nagios-Konfiguration wird nicht übernommen

Vor dem Starten und vor dem erneuten Einlesen der Nagios-Konfigurationsdateien führt der Nagios-Server eine Überprüfung der Konfigurationsdateien durch. Wird ein Fehler gefunden, startet der Nagios-Server nicht bzw. übernimmt die neuen Konfigurationsdateien nicht. Die Überprüfung lässt sich manuell mit dem Befehl

```
nagios2 -v /etc/nagios2/nagios.cfg
```

auslösen. Die Ausgaben dieses Befehls geben detaillierte Informationen über mögliche Fehler.

4.3 Der NRPE Server startet nicht mehr

Sollte sich der NRPE nach einem Neustart automatisch wieder beenden, liegt ein Fehler in der Konfiguration vor. Zunächst sollte eine manuelle Überprüfung der Konfigurationsdateien unter `/etc/nagios/` durchgeführt werden. Sollte dies keinen Erfolg bringen, kann in der Datei `/etc/nagios/nrpe.cfg` die Einstellung `debug=0` auf `debug=1` geändert werden, wodurch der NRPE Fehlermeldung in der Logdatei `/var/log/syslog` ablegt. Anschließend ist der NRPE erneut zu starten und die Datei `/var/log/syslog` auf Fehlermeldungen zu überprüfen.

4.4 Nagios-Fehlermeldung “Nagios is currently not checking for external commands”

Die Nagios-Pakete nehmen aus Sicherheitsgründen in der Standardeinstellung keine Befehle durch die Nagios-Benutzeroberfläche entgegen. Über die Univention Configuration Registry-Variable `nagios/server/checkexternalcmd` kann dieses Verhalten gesteuert werden.