

# Standardpaket

**ITdesign**

WATCH 

Version 1.5

Wien, November 2010

TAKE **IT** EASY



Konzeption und Inhalt: ITdesign

Nutzung durch Dritte nur mit schriftlicher Genehmigung von ITdesign

---

## **INHALTSVERZEICHNIS**

<b>1</b>	<b>ITDESIGN WATCH IT STANDARDPAKET .....</b>	<b>3</b>
1.1	NUTZEN FÜR DEN KUNDEN .....	3
1.2	ÜBERWACHTE ZIELSYSTEME.....	4
1.3	MESSUNGEN .....	4
1.4	SERVICE LEVEL MONITORING.....	6
1.5	BENACHRICHTIGUNGEN .....	6
1.6	REPORTS .....	6
1.7	VIEWS.....	6
1.8	MONITORING SYSTEM.....	6
1.9	SMS MODEM.....	7
<b>2</b>	<b>WARTUNGSVERTAG .....</b>	<b>8</b>
<b>3</b>	<b>LEISTUNGSBESCHREIBUNG.....</b>	<b>9</b>
3.1	PROJEKTABLAUF .....	11
<b>4</b>	<b>ABGRENZUNG UND VORGABEN .....</b>	<b>13</b>
4.1	ABGRENZUNG .....	13
4.2	VORGABEN.....	14

## 1 ITdesign WATCH IT Standardpaket

ITdesign hat ein Lösungspaket erstellt, welches zu einem Fixpreis ein zentrales Monitoringsystem auf Basis von WATCH IT zur Verfügung stellt.

In diesem Paket sind alle erforderlichen Komponenten (Lizenzen, Hardware und Dienstleistungen) enthalten, um das Monitoringsystem in dem nachfolgend definierten Umfang einzusetzen.

Ziel dieses Lösungspakets ist die Inbetriebnahme eines zentralen Überwachungssystems, welches ein Basismonitoring der unterschiedlichen Betriebssysteme und Netzwerkkomponenten beinhaltet, Benachrichtigungen bei Störungen durchführt und den Gesamtzustand der IT-Infrastruktur darstellt.

### 1.1 Nutzen für den Kunden

Für den Kunden ergibt sich mit WATCH IT folgender Nutzen:

- **Einfache und rasche Implementierung**
  - Das mit dieser Lösung aufgebaute Monitoring ermöglicht bereits nach einer Woche vollständig überwachte Systeme
  - Durch ein Agentless Monitoring entfällt der Update der Zielsysteme, die Installation des Monitoringsservers selbst genügt → geringe Kosten
- **Überwachung der Server und Netzwerklandschaft**
  - Übersichtlich aufbereitete grafische Darstellung der gemessenen Zustände auch für technisch weniger versierte Personen
  - Erkennen von Problemen bevor es zu Stillständen kommt
  - Die Korrelation von Einzelmessungen ermöglicht eine sehr gezielte Alarmierungslogik, damit die Fehlermeldungen übersichtlich bleiben
- **Überwachung von Service Level Agreements**
  - Darstellung und Berechnung von Verfügbarkeit der Systeme
  - Nachweis von Betriebsfähigkeit der Systeme
  - Die Auswertungen von WATCH IT geben Argumente bei der Diskussion mit Fachbereichszuständigen über die Verfügbarkeit
- **Konsolidierte Darstellung für das Management**
  - Darstellung der Zustände unternehmenskritischer Systeme und Dienste
  - Korrelationen von Einzelmessungen ermöglichen Darstellung eines Gesamtzustandes
- **Trendanalyse und Budgetplanung**
  - Langzeitstatistiken und grafische Darstellung von Messergebnissen erlauben Trendanalysen
  - Die Messwerte und Trendanalysen ermöglichen eine auf Fakten basierende Budgetplanung (z.B. Diskauslastungen)
- **Benachrichtigung bei Störungen**

- Per E-Mail und/oder SMS, ganz wie es die für den Betrieb Zuständigen wünschen
- Exakte und zielgerichtete Benachrichtigung verhindert Benachrichtigungsflut bei Störungen
- **Erweiterungen**
  - Die offene Erweiterbarkeit und Struktur von **WATCH IT** ermöglichen die einfache Einbindung weiterer Systeme und Messungen
  - Erweiterungen können selbständig durchgeführt werden
  - Werden Funktionen vom Monitoring gewünscht, die das Produkt (noch) nicht liefert, können diese selbständig in kurzer Zeit realisiert werden
- **Betriebssicherheit**
  - Trotz sehr genauen Monitorings sind keine Agents auf den Zielsystemen erforderlich. Damit entfällt eine mögliche Störungsquelle am Zielsystem (wer kennt nicht z.B. die Virens Scanner Software, die an allen Probleme „schuld“ ist)
  - Keine zusätzliche Belastung des Netzwerksverkehrs und Belastung der Zielsysteme

## 1.2 überwachte Zielsysteme

Folgende Systeme und Netzwerkkomponenten können in die Überwachung eingebunden werden:

- Microsoft Windows ab Version NT 4.0
- Novell Netware ab Version 6.0
- SUSE Linux ab Version 7.0
- SUN Solaris ab Version 5.7
- Red Hat Linux ab Version 6.2
- OpenBSD ab Version 3.2
- VMware ESX Server
- SNMP fähige Netzwerkkomponenten (z.B. Router, Switches,...)

Im Standardpaket ist die Einbindung von 15 Zielsystemen durch ITdesign enthalten. Die Systeme (Hostname, Servertyp, Betriebssystem) werden zum Zeitpunkt der Beauftragung definiert. Weitere Systeme können durch den Kunden selbst integriert werden.

## 1.3 Messungen

Folgende Messungen sind als Basismessungen definiert:

Messung	Beschreibung
<b>Erreichbarkeit</b>	Mittels ICMP Ping wird die Erreichbarkeit des Zielsystems überprüft
<b>System Info</b>	Die SNMP System Info und Uptime des Zielsystems wird

		ausgelesen und angezeigt
<b>CPU Auslastung</b>		Die durchschnittliche Auslastung aller CPUs wird ausgelesen und ausgewertet (system time, User time)
<b>Arbeitsspeicher</b>		Die Auslastung des virtuellen und physischen Speichers wird ausgelesen und angezeigt
<b>Kapazitätsauslastung der Volumes/Partitions</b>		Die Auslastung aller Volumes bzw. Partitions (ja nach Betriebssystem) werden ausgelesen und dargestellt (max/used)
<b>Datendurchsatz von Netzwerkports</b>		Der Datendurchsatz der Netzwerkports wird ausgelesen (in/out) und grafisch dargestellt
<b>Erkennen von Konfigurationsänderungen von Netzwerkports</b>		Die Konfiguration der Netzwerkports (speed, description, status) wird laufend gegen eine Referenzkonfiguration (Snapshot) verglichen. Änderungen werden angezeigt bzw. können als neuer Snapshot definiert werden
<b>Status von Netzwerkports</b>		Der Status von Netzwerkports (online/offline) wird überprüft und angezeigt
<b>Status von Systemprozessen</b>		Der Status der für das Betriebssystem erforderlichen Prozesse bzw. deamons wird überwacht
<b>Timeserver</b>		Die Zeitsynchronität des Zielsystems zum Zeitserver wird überprüft und eine eventuelle Differenz angezeigt.
<b>Anzahl der Prozesse</b>		Die Gesamtanzahl der Prozesse des Systems wird gemessen und dargestellt
<b>Anzahl der angemeldeten Users</b>		Eine Liste der angemeldeten interaktiven User am Zielsystem wird erstellt und angezeigt
<b>Status von MS Windows Services</b>		Der Status vom Services wird ausgelesen und angezeigt (MS Windows)
<b>Packet Receive Buffers</b>		Die Auslastung von Packet Receive Buffers wird ausgelesen und angezeigt (Novell Netware).
<b>Service Prozesse</b>		Die Auslastung von Service Prozesse wird ausgelesen und angezeigt (Novell Netware).
<b>Available Cache Buffers</b>		Auslastung von Available Cache Buffers wird ausgelesen und angezeigt (Novell Netware).
<b>Abends</b>		Die Anzahl der Abends wird ausgelesen und angezeigt (Novell Netware )
<b>Status von nlms</b>		Der Status (loaded/unloaded) von nlms wird ausgelesen und angezeigt (Novell Netware)

### 1.4 Service Level Monitoring

Die Gesamtzustände von Netzwerk- und Serverkomponenten werden als IT-Service festgelegt und sowohl in SLA Reports als auch in einer Management View dargestellt:

- Alle Netzwerkkomponenten online
- Alle Serverkomponenten online

### 1.5 Benachrichtigungen

Die Benachrichtigung bei Störungen erfolgt wahlweise per Email und/oder per SMS mittels eines im Paket enthaltenen SMS Modems. Zum Zeitpunkt der Implementierung wird die jeweilige Benachrichtigungsart festgelegt. Im Standardpaket ist die Einbindung von 3 Benutzer-Accounts für Administratoren enthalten. Weitere Accounts können durch den Kunden selbst eingerichtet werden.

### 1.6 Reports

Zusätzlich zu den Standard Reports von Nagios und **WATCH IT** werden SLA Reports für 2 IT Services eingerichtet:

- Verfügbarkeit der Serverkomponenten gesamt
- Verfügbarkeit der Netzwerkkomponenten gesamt

Weitere SLA Reports können durch den Kunden selbst eingerichtet werden.

### 1.7 Views

Zusätzlich zu der Standard Administrationsoberfläche von Nagios werden die **WATCH IT** Oberfläche inklusive Search Funktion und die **WATCH IT** Management View eingerichtet.

In der Management View werden die 2 definierten o.a. IT Services dargestellt und als WEB Oberfläche zur Verfügung gestellt. Die Darstellung erfolgt im Standard **WATCH IT** Layout. Als Web Server wird der **WATCH IT** Monitoringserver eingesetzt.

### 1.8 Monitoring System

Die nachfolgend angeführten Lizenzen und Installationskits für die Installation und den Betrieb des Monitoringserver zur Überwachung von bis zu 50 Zielsystemen sind in diesem Standardpaket enthalten.

- SUSE Linux Enterprise Server 11 for X86, AMD64 & Intel EM64T
- **WATCH IT** Lizenzen (max 50 Zielsysteme)
  - **WATCH IT** Basispaket
  - **WATCH IT** Microsoft
  - **WATCH IT** Novell
  - **WATCH IT** VMware
  - **WATCH IT** Citrix XenApp
  - **WATCH IT** End to End Messung
  - **WATCH IT** SLA Überwachung

### **1.9 SMS Modem**

Die nachfolgend angeführte Hardware für den Versand von SMS Benachrichtigungen ist in diesem Paket enthalten:

- SMS Modem Teltonika ModemUSB/GSM

## 2 **Wartungsvertrag**

Im Standardpaket ist ein Wartungsvertrag für folgende Komponenten enthalten:

- SUSE Linux Enterprise Server 10 for X86, AMD64 & Intel EM64T - e-License, 1 year subscription
- für die unter Punkt 2.8 genannten **WATCH IT** Module

Jegliche Adaptierungen am System, die vor Ort vorgenommen werden müssen, sind gesondert zu bestellen.

Die **WATCH IT** Wartung pro Jahr beträgt 25% vom Listpreis. Der Wartungspreis für das erste Jahr ist im **WATCH IT** Standardpaketpreis enthalten.

### 3 Leistungsbeschreibung

Der folgende Abschnitt beschreibt die technische Umsetzung und Konfiguration des Monitoringsystems.

- **Systeminstallation bestehend aus:**
  - Betriebssysteminstallation
  - Installation **WATCH IT**
  - Installation des SMS Modems

ITdesign unterstützt SUSE Enterprise Server als Betriebssystem für die Monitoring Station.

Auf einer vom Kunden zur Verfügung gestellten Hardware wird das Betriebssystem installiert. Die Installation erfolgt mittels automatisiertem Setup; dadurch ist kein umfassendes Unix Know How notwendig.

Das Betriebssystem wird so angepasst, dass für die Administratoren ein möglichst geringer administrativer Aufwand zum Betrieb des Systems entsteht.

- **Einrichten der Basismessungen**

Die Basismessungen werden als Template zur Verfügung gestellt und können den entsprechenden Zielsystemen zugewiesen werden. Die Messungen erfolgen rund um die Uhr (7x24). Bei Bedarf erfolgt eine Einschränkung der Fehlerbenachrichtigung durch Definition der Benachrichtigungszeiten. Die Messungen werden periodisch durchgeführt. Folgende Zeitintervalle sind vorgesehen (min) 1, 5, 15 und 60 Minuten.

Neben dem Zeitintervall wird auch die Anzahl der Wiederholungen festgelegt, bevor eine Fehlerbenachrichtigung erfolgt (Standard: 3 Wiederholungen im Minutenabstand).

- **Einbinden der Zielsysteme**

Von ITdesign werden gemeinsam mit dem Kunden 15 Zielsysteme folgender Betriebssysteme (sofern vorhanden) eingebunden.

- Microsoft Windows
- Novell Netware 6.0 oder Novell Open Enterprise Server
- Linux/Unix
- VMware
- Netzwerkkomponenten

Weitere Zielsysteme können durch den Kunden nach erfolgtem KnowHow Transfer eingebunden werden:

Um Zielsysteme einfacher, verständlicher und übersichtlicher einpflegen zu können, wird eine eigene **WATCH IT** Konfigurationsdatei verwendet.

- **Anpassung der Schwellwerte**

Schwellwerte, welche sich in der Praxis bewährt haben, werden konfiguriert und gegebenenfalls an das Kundenenvironment angepasst.

- **Implementierung einer Standard Management View (Gesamtzustand der IT Services)**

Eine Management View zur Darstellung von IT Services wird mit einer **WATCH IT** Standardvorlage aufgebaut und auf dem Monitoringserver als WEB Oberfläche zur Verfügung gestellt. Folgende IT Services werden in der Management View dargestellt:

- Alle Netzwerkkomponenten online
- Alle Serverkomponenten online

- **Einrichtung von Verfügbarkeitsauswertungen der definierten IT Services**

Für die in der Management View dargestellten IT Services werden Verfügbarkeitsreports erstellt und in die **WATCH IT** Oberfläche integriert.

- **Aufbau des Benachrichtigungssystems**

Eine Benachrichtigung erfolgt bei Schwellwertverletzungen (CRITICAL), bei nicht Erreichbarkeit eines Zielsystems und bei Wiederherstellung des Normalzustandes:

- Host DOWN
- Host UP
- Service CRITICAL
- Service RECOVERY

Es werden 2 Benachrichtigungsarten für 3 Administratoren eingerichtet. Die Benachrichtigungszeiträume werden je Benachrichtigungsart festgelegt, z.B.

- E-Mail Mo-So 0-24:00
- SMS Mo-Fr 8:00-18:00

Störungseskalationen und Wiederholungen von Benachrichtigungen werden nicht implementiert.

- **Datensicherung**

Die Sicherung des Monitoringsystems und der Messdaten erfolgt über das bestehende Backupsystem des Kunden. Entsprechende SMB Shares werden freigegeben, über welche die Daten gesichert werden können. Die Einrichtung des Backupjobs erfolgt durch den Kunden. Das Betriebssystem des Monitoringsservers wird nicht gesichert, da in der Dokumentation eine genaue Anleitung zur Wiederherstellung enthalten ist.

- **Dokumentation**

Die Dokumentation wird von ITdesign für die gesamte, im Zuge der Installation geschaffene Monitoringlösung erstellt. In der Dokumentation werden jene Details beschrieben, die über die Standarddokumentation von Nagios hinausgehen.

Die Dokumentation wird besonders für die folgenden Aufgaben benötigt:

- 1) Grundlage für den Know How Transfer

Der Tatsache, dass – wie die Erfahrung zeigt – die Erstellung von Dokumentationen oftmals vernachlässigt wird, versucht ITdesign dadurch

entgegenzuwirken, indem der weitere Verlauf des Projektes die Dokumentation voraussetzt.

2) Erweiterung der Monitoringlösung

Jede Erweiterung des Monitoringsystems wird einfach in die bereits vorhandene Dokumentation aufgenommen.

3) Nachschlagewerk für die EDV Betreuer und neue EDV-Mitarbeiter

Die EDV-Betreuer, die anhand der Dokumentation eingewiesen werden, haben ein Nachschlagewerk über ihre Systemumgebung jederzeit zur Verfügung.

Nach Abschluss des Projektes erfolgt die Wartung der Dokumentation durch Mitarbeiter des Kunden.

- **Know How Transfer**

Prinzipiell ist der Know How Transfer permanent während der Installation vorgesehen. Am Ende der Installation ist ein Workshop, mit einem halben Arbeitstag limitiert, geplant.

Die Wissensweitergabe erfolgt anhand der definierten Basismessungen an bis zu 3 vom Kunden definierte Mitarbeiter.

Nach dem Know How Transfer sollten die Administratoren des Kunden in der Lage sein, weitere Systeme eigenständig einzubinden und Basismessungen durchzuführen.

### 3.1 Projekttablauf

Das Implementierungsprojekt gliedert sich in folgende Teile auf:

- **Erstellung eines Umsetzungsplans**

In einem Kick Off Meeting wird definiert, in welcher Form die eingesetzten Systeme überwacht werden und wo der Überwachungsserver im Netzwerk zum Einsatz kommen wird. ITdesign wird im Vorfeld die für das Kick Off benötigten Informationen bekannt geben.

Themen:

- Definition der Parameter für die Systemüberwachung
- Darstellung der aktuellen Netzwerkstruktur
- Firewall, snmp, Maileinstellungen
- Definition der Administrationsberechtigungen
- Definition der Benachrichtigungswege im Fehlerfall (E-mail und/oder SMS)
- Verantwortlichkeiten der jeweiligen Projektmitarbeiter
- Umsetzungszeitplan
- Beistellungen durch den Kunden
- Testprogramme / Abläufe
- Abnahmekriterien

Weiters dient dieses Meeting auch dazu, dass alle Beteiligten die Ziele und die Rahmenbedingungen kennen lernen.

Die im Kick Off Meeting besprochenen Themen werden in Abstimmung mit den Mitarbeitern des Kunden in einem Protokoll festgehalten. Dieser Umsetzungsplan wird vom Kunden innerhalb einer Woche nach Vorlage überprüft, bei Akzeptanz abgenommen und gilt als beidseitig verbindliche Basis für die weitere Abwicklung des Projektes und als Basis für die Abnahme.

- **Kundenvorbereitungen**

Nach dem Kick Off Meeting hat der Kunde Zeit die entsprechenden Vorbereitungen in der Infrastruktur durchzuführen. Die notwendigen Schritte werden im Zuge des Kickoff Meetings besprochen und festgelegt.

- **Umsetzung**

Nach Abschluss der notwendigen Vorarbeiten des Kunden beginnt ITdesign gemeinsam mit dem Kunden mit der Umsetzung lt. Angebot bzw. Kick Off Meeting (siehe Technische Umsetzung)

- **Abschlussworkshop**

Am Ende der Installation ist der Know How Transfer, mit einem halben Arbeitstag limitiert, vorgesehen. Die Wissensweitergabe erfolgt anhand der definierten Basismessungen an bis zu 3 vom Kunden definierte Mitarbeiter.

- **Abnahme**

Die im Umsetzungsplan definierten Abnahmekriterien werden gemeinsam besprochen, überprüft und die Ergebnisse in einem Protokoll festgehalten. Das Projekt gilt als abgenommen, wenn während der Abnahme keine gravierenden Mängel erkannt werden.

## 4 Abgrenzung und Vorgaben

Im folgenden Abschnitt wird eine exakte Abgrenzung der Inhalte, die in der Pauschale enthalten sind, beschrieben. Weiters werden die benötigten Anforderungen bzw. Vorgaben für die Kundenumgebung definiert.

### 4.1 Abgrenzung

- **Integration von 15 Zielsystemen**  
Es werden 15 Zielsysteme integriert. Zusätzliche Systeme können durch den Kunden eingebunden werden
- **1 Zentraler Monitoring Server**  
Es wird nur ein Monitoringserver auf einem Standort aufgebaut. Weitere WATCH IT Monitoringserver werden durch dieses Lizenzmodell nicht unterstützt.
- **Implementierung von Basismessungen**  
Es werden nur die in diesem Dokument definierten Messungen implementiert. Zusätzlich Messungen können durch den Kunden konfiguriert und entwickelt werden.
- **Lizenz für 50 Zielsysteme**  
In diesem Paket ist die Überwachung von max 50. Zielsystemen unterstützt. Jeder Host (lt. Nagios Konfiguration) wird als Zielsystem gezählt.
- **Datensicherung**  
Die Sicherung des Monitoringsystems und der Messdaten obliegt dem Kunden. ITdesign stellt Verzeichnisfreigaben und Empfehlungen zur Datensicherung zur Verfügung.
- **Konfiguration der Zielsysteme**  
Die Aufwendungen zur Erfüllung der Voraussetzungen der Zielsysteme erfolgen durch den Kunden, u.a.
  - Konfiguration von snmp
  - Securityeinstellungen und Zugriffsberechtigungen
- **zusätzliche Erweiterungen des Monitoring**  
Aufwendungen, welche über die beschriebenen Leistungen hinausgehen, werden nach vorheriger Abstimmung gesondert in Rechnung gestellt.
- **Layout der WEB Oberflächen**  
Für die Benutzeroberflächen wird das Standard Layout verwendet. Layoutänderungen sind nicht im Paket enthalten.

## 4.2 Vorgaben

Die folgenden Voraussetzungen müssen in der Kunden Umgebung gegeben sein, um die Monitoringlösung implementieren zu können. Sind diese nicht vorhanden, muss der Kunde die entsprechenden Voraussetzungen schaffen bzw. ITdesign gesondert damit beauftragen.

- **Monitoring Server**

ITdesign geht davon aus, dass die benötigte Hardware vom Kunden zur Verfügung gestellt wird.

Bei einer Überwachung mit insgesamt bis zu 400 Messungen gelten folgende Mindestanforderungen an die Hardware:

1 Prozessor Quad Core Intel® Xeon® 5400 Series 2,5GHz), 4 GB RAM, Harddisk 100 GB abhängig von den zu sammelnden Datenmengen (Empfehlung RAID1), 1 Netzwerkkarte direkt im LAN, 1 DVD ROM Laufwerk eingebaut, Monitor, USB Schnittstelle

Für den Betrieb des SMS Modems muss der Monitoringserver eine USB Schnittstelle zur Verfügung stellen.

Vom Kunden sind zu definieren:

- Accounts und Passwörter für die interaktiven unprivilegierten Benutzer im Monitoring Server (= UNIX User)
- Passwort für den „root“ Benutzer des Monitoring Servers
- Passwort für den „monitor“ Benutzer des Monitoring Servers
- IP Adresse für den Monitoring Server
- Subnet Mask
- Default Gateway
- 2 DNS Server
- Full Qualified Domain Name
- NTP Server

- **zu überwachende Zielsysteme**

Die technische Umsetzung dieser Überwachungsparameter setzt einen oder mehrere der hier angeführten Punkte voraus:

- Alle Endsysteme erlauben ein „ping“ vom Überwachungsserver
- Auf den Endsystemen ist ein Zugriff zum snmp Server möglich. Dieser Zugriff erfolgt nur „read only“. Der hierfür benötigte „Community String“ muss bei der Installation bekannt sein. Ebenso muss es der IP Adresse des Monitoring Servers erlaubt sein, snmp Verbindungen zu diesen Endsystemen aufzubauen.
- Der Monitoring Server kann sich bei Unix Zielsystemen remote einloggen und „via ssh“ Daten aus den Endsystemen auslesen
- Die gewünschten Daten lassen sich aus dem entsprechenden Netzwerkkomponenten mittels snmp auslesen
- Zugriff auf administrative Passwörter der zu überwachenden Systeme

- **SMS Modem**

Die Verwendung der SMS (Mobiltelefon) Benachrichtigung erfolgt durch ein SMS Modem, welches in diesem Angebot enthalten ist. Der Kunde stellt eine SIM Karte eines Mobilfunkbetreibers zur Verfügung.

Es muss sichergestellt sein, dass bei Verwendung des SMS Modems im Aufstellungsbereich des Servers ein ausreichend starkes Empfangssignal des entsprechenden Mobilfunkprovidernetzes gegeben ist.

Das SMS Modem wird über eine USB Schnittstelle an den Server angeschlossen. Eine solche Schnittstelle muss daher am Monitoringserver zur Verfügung stehen.

- **Installationsvorgaben**

Der Spezialist von ITdesign benötigt für die Installation:

- Die Erlaubnis, sich mit dem mitgebrachten Notebook ins Firmennetzwerk des Kunden zu verbinden
- Ein Netzkabel und eine IP Adresse
- Der Notebook von ITdesign muss eine Zugriffsberechtigung ins Internet bekommen (http und https)

- **Firewall Einstellungen**

Wenn sich zwischen dem Monitoring Server und den zu überwachenden Endsystemen eine Firewall befindet, muss die Autorisierung seitens des Kunden vorliegen, sich vom Monitoring Server durch die Firewall zum Endsystem zu verbinden:

Verbindungen zu den Zielsystemen:

- ping
- snmp
- ssh
- etc. ...

Verbindungen zum Mail-Server, DNS-Server, NTP-Server, etc....

- smtp
- dns
- ntp

- **Wartungszugang**

Um im Zuge des Wartungsvertrages unterstützend eingreifen zu können, ist ein Wartungszugang für ITdesign erforderlich. Die Ports 50743 (ssh) und 443 (https) sind auf der Firewall entsprechend für ITdesign freizuschalten (gate.itdesign.at). Für ITdesign gibt es auf dem Monitoringserver einen eigenen Wartungsaccount mit administrativen Rechten.