

Checkliste / Vorabklärungen für die SiteAudit Installation

Bevor SiteAudit eingesetzt wird, empfiehlt es sich, die untenstehenden Information zu prüfen. Dies gewährleistet eine effiziente Installation und Betrieb von SiteAudit.

Voraussetzungen

1. Plattform

- Stellen Sie sicher, dass Ihr PC/Server die folgenden Systemvoraussetzungen erfüllt:

SiteAudit Monitor

Betriebssystem	Hardware
Windows 2003 Server	<ul style="list-style-type: none">● Pentium 4 3.2 GHz oder höher● 4 GB RAM● 200 MB freier Harddisk-Speicherplatz

SiteAudit Viewer:

Betriebssystem	Hardware
Windows XP mit SP2	<ul style="list-style-type: none">● Celeron 2.8 GHz oder höher● 4 GB RAM● 200 MB freier Harddisk-Speicherplatz

2. Datenbank

- Wenn ein SQL-Server im Netzwerk installiert ist, stellen Sie sicher, dass dieser genutzt werden kann und eine Datenbank für die Speicherung der gesammelten Daten verfügbar ist.
- Die minimalen Rechte für die Bearbeitung der Datenbank sind Owner-Rechte. Benutzer mit Owner-Rechten können Datenbank-Tabellen updaten, die Datenbank sichern und wiederherstellen oder Daten löschen (aus SiteAudit heraus). Mindestens eine Person, die SiteAudit benutzt, sollte diese Rechte haben.
- Um eine Datenbank zu erstellen (aus SiteAudit heraus) muss der Benutzer SA-Rechte (wenn SQL Security genutzt wird) oder Administratoren-Rechte, wenn die integrierte Security genutzt wird.

Windows Services

3. Windows Services Einstellungen:

Service	Wird wo verwendet	Start Modus
COM+ Event System	SiteAudit Monitor Ziele, welche gescannt werden sollen	Automatisch auf Servern Manuell auf Arbeitsplätzen
Remote Access Auto Connection Manager	SiteAudit Monitor und SiteAudit Viewer	Manuell
Remote Access Connection Manager	SiteAudit Monitor und SiteAudit Viewer	Manuell
Remote Procedure Call (RPC)	SiteAudit Monitor und SiteAudit Viewer	Manuell
Remote Procedure Call (RPC) Locator	SiteAudit Monitor und SiteAudit Viewer	Manuell
Remote Registry	SiteAudit Monitor	Automatisch
Server	SiteAudit Monitor und SiteAudit Viewer	Automatisch
Windows Management Instrumentation	SiteAudit Monitor Ziele, welche gescannt werden sollen	Automatisch
Windows Management Instrumentation Driver Extensions	SiteAudit Monitor	Manuell
Workstation	SiteAudit Monitor und SiteAudit Viewer	Automatisch

- Stellen Sie sicher, dass der Windows Management Instrumentation Zugang (WMI) an jedem Arbeitsplatz-Computer eingeschaltet ist, an welchem lokale Drucker angeschlossen sind und welche gescannt werden sollen und auf dem Host, auf welchem der SiteAudit Server läuft.

Ermittlung der Konfiguration

4. Netzwerk-Ermittlung :

- Erfassen Sie eine Liste der Netzwerksegmente, welche auf Drucker gescannt werden soll. Die Netzwerk-Adresse und Maske für jedes Netzwerk sind dafür erforderlich.
- Erstellen Sie eine Liste der Netzwerke, welche nicht gescannt werden sollen. Die Netzwerk-Adresse und Maske für jedes Netzwerk sind dafür erforderlich.
- Erstellen Sie die Liste der Bereiche, welche einbezogen oder ausgeschlossen werden sollen.
- Entscheiden Sie, ob Broadcasts genutzt werden sollen. Wenn Broadcasts nicht genutzt werden, fügen Sie die Broadcast Adressen zu der Liste der nicht zu scannenden Devices.
- In der Device-Tabelle, fügen Sie jegliche Devices hinzu, welche einbezogen oder ausgeschlossen werden soll. Devices welche ausgeschlossen werden sollen sind UPS Devices, DNS Server und andere Devices, auf welche nicht zugegriffen werden soll.

5. **SNMP:**

- Stellen Sie sicher, dass alle benötigten Community Strings verfügbar sind.
- Ordnen Sie die Liste in der SiteAudit-Konfiguration um sicherzustellen, dass die meistbenötigten Community Strings die ersten sind, worauf zugegriffen wird.
- Entfernen Sie alle Community Strings welche nicht benötigt werden.

6. **Windows Hosts:**

- Stellen Sie sicher, dass alle benötigten Zugriffsberechtigungen in der Liste auf Host Credentials Tabelle der Discovery Configuration Dialog Box sind.
- Stellen Sie sicher, dass jeglicher Firewall Zugriff konfiguriert wurde.

7. **Security**

- Prüfen Sie, ob SiteAudit in der Security-Software auf die White List gesetzt werden muss, damit nicht falsche Informationen registriert werden, wenn SiteAudit das Netzwerk scannt und Daten sammelt.