Checkliste vor der Bereitstellung und bei der Bereitstellung

|  |  |  |
| --- | --- | --- |
| Referenznummer **AA-00904** Views: **134** Letzte Aktualisierung: **01-29-2016 08:17** | **0 Bewertung**/Wähler | https://support.netaphor.com/admin/images/local/FirstTheme/ico-rating-g.gifhttps://support.netaphor.com/admin/images/local/FirstTheme/ico-rating-g.gifhttps://support.netaphor.com/admin/images/local/FirstTheme/ico-rating-g.gifhttps://support.netaphor.com/admin/images/local/FirstTheme/ico-rating-g.gifhttps://support.netaphor.com/admin/images/local/FirstTheme/ico-rating-g.gif |

**Vor der Bereitstellung**

| **Thema** | **Maßnahme** | **Beschreibung/Zusätzliche Hinweise** |
| --- | --- | --- |
| Infrastruktur |  |  |
| Serverhardware | Prüfung der Hardwareanforderungen basierend auf den technischen Daten von SiteAudit | Grundsätzlich gilt: Je größer die Anzahl der Geräte, umso leistungsstärker sollte die für den DCA erforderliche Serverhardware sein. |
| Software | Prüfung der Softwareanforderungen basierend auf den technischen Daten von SiteAudit | .NET 4.5.1, Windows 8.x/10/Server 2008, 2012 |
| Datenbank | SQL Server-Datenbank muss für SA verfügbar sein | Mindestens der Zugang zu DB\_OWNER muss bereitgestellt werden.  Datenbank kann vor der Installation oder bei der Installation erstellt werden.  SQL Server 2008/2012/2014 werden unterstützt |
| Erkennung |  |  |
| Scanliste Netzwerk | Netzwerklisten beziehen, um Bereiche und individuelle IP-Adressen in die Erkennung einzuschließen. | Diese Information wird normalerweise von einem Netzwerkadministrator bereitgestellt.  Die Liste kann in eine Datei eingefügt werden, die in SiteAudit importiert wird. |
| Ausschlussliste Netzwerk | Netzwerklisten beziehen, um Bereiche und individuelle IP-Adressen in die Erkennung einzuschließen. | Typische Geräte, die ausgeschlossen werden, sind UPS-Geräte, DNS-Server, Mailserver, Router und Switche. |
| SNMP Community String(s) | Read Community Strings anfordern | Netzwerkadministratoren verfügen normalerweise über diese Informationen.  Allgemeine Standards sind vorab ausgefüllt.  In den Drucker-Webseiten sind die Community String(s) enthalten.  Community String kann importiert werden. |
| Lokal angeschlossene Drucker | Anmeldeinformationen für den Zugang anfordern | Anmeldeinformationen müssen den Remote-Zugang zu den  WMI -Objekten erlauben.  Normalerweise werden die Anmeldeinformationen des Domain-Administrators reichen.  Diese Informationen können nicht importiert werden und müssen an der Maschine eingegeben werden, an der der DCA laufen wird. |
| Sicherheit |  |  |
| Protokollzugang | Die Protokolle, die SiteAudit verwendet, – SNMP, WMI, CPCA, NPAP, HTTP – müssen erlaubt sein. | Firewall(s) müssen dem SA DCA erlauben, die zuvor beschriebenen Protokolle zu verwenden.  Für den WMI -Zugang müssen lokale Hosts WMI -Zugang erlauben. |
| Whitelisting | Der SA DCA sollte in der Whiteliste aufgeführt sein, damit er nicht blockiert wird. | Während der Erkennung erscheint SA DCA als ein Portscanner für die Sicherheitssoftware.  Um das zu verhindern, sollte er in der Whiteliste aufgeführt sein. |
| Sonstiges |  |  |
| Mail-Server | SMTP-Serverkonfiguration beziehen | SMTP-Server wird verwendet, um Benachrichtigungen und planmäßige Berichte zu senden. |
| Abteilungshierarchie | Organisationsdetails beziehen (physikalisch/logisch) | Organisationsinformationen können importiert werden.  Geräte können automatisch einem Teil der Organisation zugeordnet werden, wenn das Netzwerk entsprechend organisiert ist. |

**Berichterstellung und Benachrichtigung**

| **Thema** | **Maßnahme** | **Beschreibung/Zusätzliche Hinweise** |
| --- | --- | --- |
| Berichterstellung |  |  |
| Inhalt | Entscheiden Sie über Inhalt, Zustellung und Zeitplan der Berichte.  Entscheiden Sie auch, wer welche Berichte wann erhält. | Berichte, die auf Ansichtsdateien basieren, können per E-Mail geplant und zugestellt oder an einem bestimmten Ort abgelegt werden. |
| Analyzer | Legen Sie das Inhalts- und Berichtsformat (XLSX oder PPTX) fest. | Berichte können geplant oder bedarfsgesteuert ausgeführt werden.  SiteAudit Analyzer mit Designer-Modus kann für die Erstellung neuer Berichte verwendet werden. |
| Visualizer | Grundrisse und Gerätestandorte anzeigen | SA-Daten können über einen Update der Datenquelle auf einen Grundriss upgedated werden. |
| Benachrichtigungen |  |  |
| Regeln | Legen Sie fest, welche Art von Benachrichtigungen erforderlich sind.  Stellen Sie sicher, dass die Mailserverkonfiguration korrekt ist. | Benachrichtigungen können per E-Mail an eine Person oder an ein Helpdesk geliefert und für das System angepasst werden. |
| Schwellwerte | Schwellwerte für Verbrauchsmaterialien  können für Geräte und Ebenen festgelegt werden | Benachrichtigungen können nach Schwellwertberichten ausgegeben werden.  Schwellwerte für Zugriffs-berechtigungen sind hilfreich, wenn die Kommunikation mit einem Gerät verloren gegangen ist.  Schwellwerte für MAC sind hilfreich um zu wissen, ob Geräte erkannt oder verschoben worden sind. |
|  |  |  |
| Benachrichtiger | Legen Sie fest, ob ein ein separater Host für Benachrichtigungen verwendet werden soll. | Benachrichtigungen können auf einem separaten Host laufen, um die Ressourcen des DCA-Hosts ausschließlich für Überwachungszwecke zu maximieren. |
| Andere |  |  |
| Plug-ins | Informationen über Plug-ins vom Provider beziehen | Plug-ins besitzen häufig URL-Anmeldeinformationen und einen Zeitplan, nach dem die Daten hochgeladen werden sollen. |
| BackOffice Services | BackOffice Serverinformationen beziehen | BackOffice Server besitzen häufig URL-Anmeldeinfor-mationen und einen Zeitplan, nach dem die Daten hochgeladen werden sollen. |