

ViewStation-Lizenzmanager

Best Practice



Die in diesem Dokument beschriebenen Software-Programme und enthaltenen Informationen sind vertrauliche und urheberrechtlich geschützte Produkte der KISTERS AG oder seinen Lizenzgebern. Die KISTERS-AG erlaubt lizenzierten Software-Anwendern, Teile der Dokumentation zum persönlichen Gebrauch auf Papier auszudrucken. Diese Dokumentation darf an Personen, die nicht Teil des Lizenznehmer-Unternehmens sind, weder verkauft, verteilt oder auf andere Weise vervielfältigt und weitergegeben werden.

Durch Vervielfältigung jeglicher Teile der Dokumentation verpflichtet sich der Empfänger, alles in seiner Macht stehende zu tun, um eine nicht autorisierte Verwendung und Verteilung der urheberrechtlich geschützten Informationen zu vermeiden.

Jede Art der Vervielfältigung, sei es graphisch, elektronisch oder mechanisch - eingeschlossen Fotokopieren, Aufnahmen oder Nutzung von Speicher- und Abrufsystemen - bedarf des Einverständnisses des Herausgebers.

Die KISTERS AG behält sich das Recht vor, Spezifikationen und andere in dieser Veröffentlichung enthaltenen Informationen ohne vorherige Ankündigung abzuändern.

Die KISTERS AG übernimmt keine Garantie bezüglich dieses Materials, einschließlich - wenn gleich nicht beschränkt auf - einer Garantie für die Gebrauchstauglichkeit für einen bestimmten Zweck.

Die KISTERS AG haftet nicht für Schäden (einschließlich aber nicht begrenzt auf entgangene Gewinne), die direkt oder indirekt aus der Benutzung der Dokumentation, der enthaltenen Informationen oder des Programms und des gegebenenfalls mitgelieferten Quell-Codes entstehen, auch wenn die KISTERS AG über die Möglichkeit solcher Schäden informiert ist.

Fehler innerhalb von KISTERS-Produkten sollten direkt an KISTERS gemeldet werden; wir sichern eine schnellstmögliche Bearbeitung zur Fehlerbehebung zu.

Die in diesem Dokument erwähnten Produkte können Markenzeichen und/oder gesetzlich geschützte Markenzeichen der jeweiligen Eigentümer sein. Der Herausgeber und der Autor erheben keinen Anspruch auf diese Markenzeichen.

Copyright 2024 KISTERS AG
Internet: viewer.kisters.de
E-Mail: support-viewer@kisters.de
Tel.: +49 (0) 2408 9385-360

Autor: KISTERS AG
Druckdatum der aktuellen Auflage: 16/05/2024
Aktuelle Programmversion: 2021.0

The logo for KISTERS, featuring a stylized 'K' symbol followed by the word 'KISTERS' in a bold, sans-serif font.

Inhaltsverzeichnis

Teil I	Lizenzserver-Installation	4
Teil II	Server-Konfiguration	6
Teil III	Konfiguration von Berechtigungsregel	10
Teil IV	Lizenzüberwachung	16
Teil V	Fehlerbehebung	18



Kapitel I:

Lizenzserver-Installation



1 Lizenzserver-Installation

Gehen Sie wie folgt vor, um den VS-Lizenzmanager zu installieren:

- Laden Sie das [VS Lizenzmanager ZIP-Archiv](#) herunter.
- Verschieben Sie den Inhalt des ZIP-Archivs in ein Verzeichnis Ihrer Wahl, zum Beispiel `C:\Kisters\VSIM`.
- Kopieren Sie die Lizenzdatei `VSIM.lic`, die Sie per E-Mail erhalten haben, in das Verzeichnis Ihrer Wahl neben die Datei `VSIM.exe`.
- Um den VS-Lizenzmanager auszuführen, doppelklicken Sie mit Administratorrechten auf `VSIM.exe`. Dies öffnet eine Konsole mit einem Protokoll aller VS-Lizenzmanager-Ereignissen. Das Schließen der Konsole stoppt den VS-Lizenzmanager.
- Wenn Sie Fehlermeldungen sehen, in denen Ports erwähnt werden, öffnen Sie die erforderlichen lokalen Ports in der Windows-Firewall. Die Voreinstellungen sind 6200 und 6280. Das Protokoll ist TCP. Wenn Sie eine Firewall eines Drittanbieters verwenden, können Sie diese Meldungen ignorieren. Überprüfen Sie die Ports entsprechend.
- Konfigurieren Sie den VS-Lizenzmanager nach Bedarf, siehe [Serverkonfiguration](#). Legen Sie zum Beispiel ein Admin-Passwort für die Lizenzüberwachung fest.
- Entfernen Sie den Unterstrich aus `_ServerConfig.json`, um die Konfigurationsdatei zu aktivieren.
- Starten Sie den VS-Lizenzmanager neu, damit die neue Konfiguration wirksam wird.

Als Windows-Dienst ausführen

- Um den VS-Lizenzmanager als Windows-Dienst zu installieren und auszuführen, führen Sie die Datei `windows_service_install.bat` mit Administratorrechten aus. Damit wird der Dienst so konfiguriert, dass er nach einem Systemneustart automatisch startet.
- Führen Sie nach dem Aktualisieren von `VSIM.lic` oder `ServerConfig.json` die Datei `windows_service_restart.bat` mit Administratorrechten aus, um die Änderungen auf den VS-Lizenzmanagerdienst anzuwenden.
- Um den Windows-Dienst zu entfernen, führen Sie `windows_service_uninstall.bat` mit Administratorrechten aus.

Beachten Sie: Wenn Sie den VS-Lizenzmanager mit einem 3DViewStation WebViewer auf demselben Host-System verwenden, müssen Sie ihn als Abhängigkeit zum 3DViewStation WebViewer Windows-Dienst hinzufügen. Dies gewährleistet eine korrekte Startsequenz, wenn das System neu gestartet wird.



Kapitel II:

Server-Konfiguration

2 Server-Konfiguration

Das Verhalten des VS Lizenz Managers kann über eine JSON-Datei konfiguriert werden. Zusätzlich zu den allgemeinen Einstellungen des Servers können auch die Nutzungsberechtigungen und die Zugriffsberechtigungen auf Funktionen geregelt werden. Um die Konfiguration zu ändern, bearbeiten Sie einfach die Datei `ServerConfig.json` mit einem Texteditor wie unten beschrieben. Starten Sie den VS-Lizenzmanager neu, damit die Änderungen wirksam werden.

Beachten Sie: Wenn in Dateipfaden oder Benutzernamen Sonderzeichen verwendet werden, muss JSON-Datei UTF-8-kodiert sein.

► Allgemeine Einstellungen

Ports

Die Kommunikation zwischen dem VS-Lizenzmanager und den 3DViewStation-Clients erfolgt über das TCP-Netzwerkprotokoll. Die Einstellung `TCP_PORT` definiert den verwendeten Port:

```
"TCP_PORT": 6200,
```

Der [Lizenz-Monitor](#), die Weboberfläche des VS-Lizenzmanagers, kann über einen Webbrowser aufgerufen werden: `<Adresse des Lizenzservers>:<HTTP_PORT>`. Die Einstellung `HTTP_PORT` bestimmt den verwendeten HTTP Port:

```
"HTTP_PORT": 6280,
```

Beachten Sie:

- Die angegebenen lokalen Ports müssen in der Firewall des Servers geöffnet sein, damit der VS-Lizenzmanager ordnungsgemäß funktioniert. Für beide Ports ist das erforderliche Protokoll TCP.
- Wenn Sie andere Ports als die Voreinstellung verwenden, teilen Sie uns dies bitte mit, damit wir Ihre Lizenz auf dem neuesten Stand halten können. Senden Sie dazu eine E-Mail an orders-viewer@kisters.de mit Ihrem Servernamen, dem von Ihnen verwendeten TCP-Port und der Seriennummer Ihrer Lizenz.

Passwörter

Um auf die Admin-Ansicht des Lizenz-Monitors (einschließlich Logs, Konfigurationsübersicht und Checkout-Historie) zuzugreifen, muss ein Passwort konfiguriert werden:

```
"ADMIN_PASSWORD": "SuperUser123",
```

Beachten Sie: Das Passwort wird nur in base64-Kodierung gesendet. Wählen Sie daher ein eindeutiges Passwort, das nur für den VS-Lizenzmanager verwendet wird.

Sie können optional ein Hauptpasswort konfigurieren. Wenn diese Einstellung aktiviert ist, wird sogar der einfache Lizenz-Monitor vor der Anzeige von Informationen ein Passwort abfragen:

```
"MAIN_PASSWORD": "",
```

Log-Datenerfassung

Der Speicherort der Protokolldateien des VS-Lizenzmanagers kann mit dem Parameter `LOG_PATH` geändert werden. Der Pfad kann absolut oder relativ mit einem führenden `./` sein:

```
"LOG_PATH": "./Logs",
```

Das Format der Logs kann mit dem gleichnamigen Parameter angegeben werden:

```
"LOG_FORMAT": "NORMAL",
```

Das alternative Protokollformat zu NORMAL ist RESTRICTED, das das Schreiben von Benutzernamen, Host-Namen und IP-Adressen in die Protokolldatei und deren Anzeige im Lizenz-Monitor unterdrückt. Für Support-Fälle ist es möglich, die letzten Log-Dateien über eine Schaltfläche im Lizenz-Monitor von einem normalen in ein eingeschränktes Format zu konvertieren.

Sie können die Anzahl der Tage konfigurieren, nach denen alte Log-Dateien entfernt werden:

```
"LOG_ARCHIVE_COUNT": 90,
```

Die Voreinstellung ist 90 Dateien, was 90 Tagen oder 3 Monaten entspricht. Wenn Sie das Löschen von Log-Dateien deaktivieren möchten, setzen Sie den Wert auf null.

► Erweiterte Einstellungen

Hochverfügbare Lizenzierung (HAL)

Um eine ausfallsichere Lizenzierung zu gewährleisten (z.B. bei Serverausfällen oder Updates), können Sie redundante Server einrichten, die alle dieselben Lizenzen und Funktionen bedienen können. Die Server-Adressen werden wie der Wert `LicenseServerAddress` in der Client-Lizenz `3DVS.lic` definiert:

```
"HAL_SERVERS": "6200@server01;6200@server02;6200@server03",
```

Die Reihenfolge der Server bestimmt die Priorität der Verfügbarkeit. Der erste Server sollte also der Hauptserver mit der höchsten Verfügbarkeit sein. Wenn ein Server ausfällt, übernimmt der nächste Server in der Liste die Aufgabe, solange der andere Server nicht verfügbar ist. Die Ausleihfunktion ist nur auf dem Hauptserver verfügbar und steht während der Ausfallzeit des Hauptservers nicht zur Verfügung. Unsere HAL-Konfiguration unterstützt zwei oder mehr Server, die Standardeinstellung sind drei.

Beachten Sie:

- Die Liste muss für alle Server-Konfigurationen und Client-Lizenzen identisch sein. Andernfalls tritt ein undefiniertes Verhalten auf.
- Bitte informieren Sie uns über Änderungen in Ihrer HAL-Konfiguration, damit Ihre Lizenz auf dem neuesten Stand bleibt. Senden Sie dazu eine E-Mail an orders-viewer@kisters.de mit den Namen Ihrer Server, den ausgewählten Ports und der Seriennummer Ihrer Lizenz.

Internet-Protocol-Version

Der VS-Lizenzmanager unterstützt beide Versionen des Internetprotokolls (IPv4 oder IPv6). Welche Sie bevorzugen, können Sie hier festlegen:

```
"IP_VERSION": "IPv4",
```

Einstellungen für den Verlauf

Die Verlaufsdaten (maximale Nutzung und Ablehnungen) werden häufig aktualisiert, aber standardmäßig nur alle acht Stunden, um die Serverlast zu reduzieren. Dies kann in den Einstellungen geändert werden:

```
"HISTORY_UPDATE_HOURS": 8,
```

Ähnlich wie bei der Bereinigung des Archivs der Log-Dateien ist es möglich, alte Verlaufsdaten automatisch zu entfernen. Dies umfasst nur Echtzeitdaten, die den größten Teil des Speicherplatzes für Verlaufsdaten einnehmen. Diese Einstellung ist standardmäßig deaktiviert:

```
"HISTORY_ARCHIVE_COUNT": 0,
```

Heartbeats und Timeouts

Um die kontinuierliche Nutzung von ausgecheckten Funktionen sicherzustellen, verwendet der VS-Lizenzmanager Heartbeats.

- Verwenden Sie `HEARTBEAT_SECONDS`, um zu konfigurieren, wie oft Heartbeats von Clients gesendet werden. Die Voreinstellung ist 2 Minuten und 20 Sekunden.
- Mit `TIMEOUT_SECONDS` können Sie konfigurieren, wann ein Client eine Zeitüberschreitung nach dem erfolgreichen Empfang des letzten Heartbeats erhalten soll. Die Voreinstellung ist 5 Minuten.
- Verwenden Sie `HEARTBEAT_CONTROL_SECONDS`, um zu konfigurieren, wie oft der Server auf Heartbeats der Clients prüft. Die Voreinstellung ist 3 Sekunden. Wenn Sie eine große Anzahl von Clients haben, kann dieser Wert leicht erhöht werden, um die Serverlast zu verringern.

In der Konfigurationsdatei sehen diese Werte wie folgt aus:

```
"HEARTBEAT_SECONDS": 140,  
"TIMEOUT_SECONDS": 300,  
"HEARTBEAT_CONTROL_SECONDS": 3,
```

Kapitel III:

Konfiguration von Berechtigungsregel

3 Konfiguration von Berechtigungsregel

Die Nutzungsberechtigungen des VS-Lizenzmanagers können durch Bearbeiten und Speichern der Datei `ServerConfig.json` konfiguriert werden. Dies beinhaltet das Zulassen, Verweigern, Einschränken und Reservieren von Checkouts und Ausleihen von Funktionen für bestimmte Benutzer. Starten Sie den VS-Lizenzmanager neu, damit die Änderungen wirksam werden.

Wann sollte ich welche Berechtigungsregel verwenden?

- Wenn Sie möchten, dass die meisten Ihrer Benutzer alle Features nutzen können und nur einige wenige eingeschränkt sind, verwenden Sie [Deny-Regeln](#)^[14].
- Wenn Sie einigen wenigen privilegierten Benutzern die Nutzung bestimmter Features erlauben und die meisten Ihrer Benutzer einschränken möchten, verwenden Sie [Allow-Regeln](#)^[12].
- Wenn Sie die Anzahl der Features, die verschiedenen Benutzergruppen zur Verfügung stehen, kontrollieren möchten, verwenden Sie [Limit-Regeln](#)^[14] und [Reserve-Regeln](#)^[15].

Wie kann ich bestimmte Benutzer angeben?

In jeder Regel können Benutzer mit Benutzernamen, Hostnamen oder IP-Adressen (IPv4 oder IPv6) angegeben werden und müssen durch ein Semikolon getrennt werden:

```
"USERS": "BenutzerEins;BenutzerZwei;BenutzerDrei;..."
```

Wenn die Liste umfangreich wird oder wenn dieselbe Liste in mehreren Berechtigungsregeln verwendet wird, ist es sinnvoll, am Ende der Konfigurationsdatei Gruppen (GROUPS) zu definieren. Das Format zur Definition der Gruppenmitglieder (MEMBERS) ist das gleiche wie für USERS. Geschweifte Klammern {...} definieren eine Gruppe innerhalb der Gruppenliste [...], getrennt durch Kommata.

```
"GROUPS": [
  {
    "NAME": "Gruppe 1",
    "MEMBERS":
    "BenutzerEins;BenutzerZwei;BenutzerDrei;...;BenutzerN"
  },
  {
    "NAME": "Gruppe 2",
    "MEMBERS": "Host01;Host02;Host03;...;HostX"
  }
]
```

Sie können Benutzer jetzt wie folgt angeben:

```
"USERS": "Gruppe 1;Gruppe 2"
```

Beachten Sie:

- Wenn Sie viele Hostnamen oder IP-Adressen einschränken, können Sie Platzhalter wie „4.3.2.*“ oder „PC*“ oder IP-Bereiche wie „4.3.2.10–50“ verwenden. Beispiele für die Verwendung finden Sie unten.
- Unter Windows können Sie Ihre lokalen Gruppen verwenden. Wenn Sie eine lokale Gruppe „Meine Benutzer“ haben, die eine Liste von Domänenbenutzern oder eine Domänenbenutzergruppe enthält, können Sie diese wie einen Benutzer- oder Gruppennamen in der Konfigurationsdatei verwenden, indem Sie ihr einfach ein „&“ voranstellen: "USERS" : "&Meine Benutzer". Beispiele für die Verwendung finden Sie unten.

Wichtige Syntax-Regeln:

- Die Serverkonfigurationsdatei verwendet die standardmäßige JSON-Syntax.
- Eckige Klammern [...] definieren die Liste der Berechtigungsregeln für eine Berechtigungseinstellung, getrennt durch Kommata.
- Geschweifte Klammern {...} definieren eine einzelne Berechtigungsregel, die durch Kommata getrennt ist.
- Mehrere Schlüssel-Wert-Paare innerhalb einer Berechtigungsregel müssen ebenfalls durch Kommas getrennt werden.
- Alle Benutzer, Features und Seriennummern müssen durch ein Semikolon getrennt werden.

- Sie können die folgenden Beispiele als Vorlagen verwenden.

Allow-Regeln

Die Regeln `ALLOW_CHECKOUTS` und `ALLOW_BORROWS` schränken die Nutzung von Features auf alle außer den angegebenen Benutzern ein. Wenn Sie also berechnete Benutzer haben, verwenden Sie diese Einstellungen. Sie bestehen aus drei Schlüsselwörtern:

- `USERS`: erforderlich, Liste der Benutzernamen oder Hostnamen, IP-Adressen oder Gruppennamen
- `FEATURES`: optional, Liste der zu beschränkenden Features
- `SERIALNUMMERN`: optional, die betroffenen Lizenz-/Seriennummern (nur erforderlich, wenn Sie mehrere Lizenzen auf einem VS-Lizenzmanager verwenden)

Beachten Sie: Die optionalen Schlüsselwörter `FEATURES` und `SERIALNUMMERN` können entfernt, leer gelassen oder auf `*` gesetzt werden, wenn sie nicht verwendet werden.

Beispiele

Eine Regel, die Funktionen nur für ausgewählte Benutzer zulässt, würde wie folgt aussehen:

```
"ALLOW_CHECKOUTS": [
  {
    "FEATURES":
"FUNCTIONALITY_ADVANCED_ANALYSIS;FUNCTIONALITY_TECHDOC",
    "USERS": "Ein Benutzer; Ein anderer Benutzer; Ein
weiterer Benutzer"
  }
],
```

Das Ausleihen von `EXPORT_ALL` nur für die in einer Group mit dem NAMEN „Benutzer-Ausleihen“ definierten Members zuzulassen, würde so aussehen:

```
"ALLOW_BORROWS": [
  {
    "FEATURES": "EXPORT_ALL",
    "USERS": "Benutzer-Ausleihen"
  }
],
...
"Groups" : [
  {
    "NAME": "Benutzer-Ausleihen",
    "MEMBERS": "Ein Benutzer; Ein anderer Benutzer; Ein
weiterer Benutzer"
  }
]
```

Dieselbe Regel, aber mit der Einschränkung, dass alle Features für alle Benutzer außer den Mitgliedern der definierten Gruppe ausgeliehen werden können:

```
"ALLOW_BORROWS": [
  {
    "USERS": "Benutzer-Ausleihen"
  }
],
```

Mehrere zulässige Regeln werden durch ein Komma getrennt:

```
"ALLOW_CHECKOUTS": [
  {
    "FEATURES":
"FUNCTIONALITY_ADVANCED_ANALYSIS;FUNCTIONALITY_TECHDOC",
    "USERS": "Benutzer-Funktionen"
  },
  {
    "FEATURES": "KAS",
    "USERS": "KAS-Benutzer"
  }
],
```

Wenn Sie ein Feature nur für eine bestimmte Windows-Benutzergruppe mit dem Präfix & zulassen, sieht das folgendermaßen aus:

```
"ALLOW_CHECKOUTS": [
  {
    "FEATURES": "EXPORT_ALL",
    "USERS": "&WindowsGruppe"
  }
],
```

Wenn Sie ein Feature für ein bestimmtes Hostnamenmuster zulassen, sieht das folgendermaßen aus. Dies würde alle PC's mit Namen wie PC001 und PC456 oder WS12CAD und WS34CAD erlauben.

```
"ALLOW_CHECKOUTS": [
  {
    "FEATURES": "EXPORT_ALL",
    "USERS": "PC*;WS*CAD"
  }
],
```

Eine der Mehrfachlizenzen nur für eine bestimmte IP-Domäne zuzulassen, würde so aussehen:

```
"ALLOW_CHECKOUTS": [
  {
    "SERIALNUMBERS": "2024-0101-123456",
    "USERS": "4.3.2.*"
  }
],
```

Wenn Sie eine Lizenz nur für einen bestimmten IP-Bereich zulassen, sieht das folgendermaßen aus:

```
"ALLOW_CHECKOUTS": [
  {
    "USERS": "4.3.2.10-50"
  }
],
```

Deny-Regeln

Die Deny-Regeln `DENY_CHECKOUTS` und `DENY_BORROWS` schränken die Nutzung von Funktionen auf die angegebenen Benutzer ein, so dass die meisten Benutzer sie trotzdem nutzen können. Die Syntax und die Schlüsselwörter sind dieselben wie bei den Regeln für Allow.

Beispiele

Eine Regel, die ausgewählten Benutzern Funktionen verweigert, würde wie folgt aussehen:

```
"DENY_CHECKOUTS": [
  {
    "FEATURES":
"FUNCTIONALITY_ADVANCED_ANALYSIS;FUNCTIONALITY_TECHDOC",
    "USERS": "Ein Benutzer; Ein anderer Benutzer; Ein
weiterer Benutzer"
  }
],
```

Eine Regel, die das Ausleihe von `EXPORT_ALL` für die in einer Group mit dem NAMEN "Ausleihe verweigert" definierten Members verweigert, würde wie folgt aussehen:

```
"DENY_BORROWS": [
  {
    "FEATURES": "EXPORT_ALL",
    "USERS": "Ausleihe verweigert"
  }
],
...
"Groups" : [
  {
    "NAME": "Ausleihe verweigert",
    "MEMBERS": "Ein Benutzer; Ein anderer Benutzer; Ein
weiterer Benutzer"
  }
]
```

Beachten Sie:

- Gleichzeitig schränken die Checkout-Regeln auch die Ausleih-Vorgänge ein, aber die Borrow-Regeln haben keinen Einfluss auf die Checkout-Aktionen.
- Deny-Regeln haben Vorrang vor allen Allow-Regeln. Wenn ein Benutzer für dieselbe Lizenz und dieselbe Funktion sowohl in einer Allow- als auch in einer Deny-Regeln aufgeführt ist, wird die Deny-Regel angewendet und die Allow-Regel ignoriert.

Limit-Regeln

Die Limit-Regeln `LIMIT_CHECKOUT` und `LIMIT_BORROW` sind nützlich, um die Anzahl der Funktionen zu steuern, die für verschiedene Benutzergruppen verfügbar sein sollen. Sie werden auch verwendet, um die Dauer des Ausleihens von Funktionen zu begrenzen. Ihre Syntax basiert auf den Allow- und Deny-Regeln, mit zusätzlichen Schlüsselwörtern:

- `COUNT`: Die Anzahl der Features, die für die angegebenen `USERS` verfügbar sein sollen.
- `EXCEPT_USERS`: Es ist möglich, Ausnahmen zu einer Limit-Regel hinzuzufügen. Wenn Sie also berechnete Benutzer innerhalb einer größeren Gruppe haben, die Sie einschränken möchten, fügen Sie sie hier hinzu.

Nur für `LIMIT_BORROW`:

- `HOURS`: Die maximale Anzahl von Stunden, die die angegebenen Funktionen ausgeliehen werden können.

Beispiele

Schränken Sie die Nutzung eines Features innerhalb einer Gruppe von Benutzern ein:

```
"LIMIT_CHECKOUTS": [
  {
    "FEATURES": "IMPORT_ALL",
    "USERS": "Benutzer 1;Benutzer 2; Benutzer
3;...;Benutzer 30",
    "COUNT": 15
  }
],
```

Begrenzen Sie die Ausleihdauer einer Funktion für alle Benutzer auf eine Woche, mit Ausnahme eines berechtigten Benutzers, der drei Monate lang ausleihen darf. Dies wird erreicht, indem Sie zunächst die Voreinstellung auf drei Monate erhöhen und dann alle Benutzer mit Ausnahme des berechtigten Benutzers einschränken:

```
"LIMIT_BORROWS": [
  {
    "HOURS": 2160
  },
  {
    "EXCEPT_USERS": "Berechtigter Benutzer",
    "HOURS": 168
  }
],
```

Reserve-Regeln

Die Reserve-Regel `RESERVE_CHECKOUTS` kann im Gegensatz zu den [Limit-Regeln](#)^[14] verwendet werden, um sicherzustellen, dass eine bestimmte Anzahl an Funktionen für bestimmte Benutzer immer verfügbar ist. Die Syntax ist die gleiche wie bei [Allow-Regeln](#)^[12], mit dem Zusatz des Schlüsselworts `COUNT`.

Beispiele

Reservieren Sie eine Funktion für drei berechtigte Hosts:

```
"RESERVE_CHECKOUTS": [
  {
    "FEATURES": "IMPORT_2D_ADVANCED",
    "USERS": "HostX;HostY;HostZ",
    "COUNT": 3
  }
],
```



Kapitel IV:

Lizenzüberwachung

4 Lizenzüberwachung

Der Lizenz-Monitor, die Weboberfläche des VS-Lizenzmanagers, kann über einen Webbrowser aufgerufen werden: `<Adresse des Lizenzservers>:<HTTP_PORT>`. Sie zeigt Lizenzinformationen, die Verfügbarkeit und Nutzung von Funktionen und die verbundenen Clients an. Die Lizenzüberwachung wird automatisch alle 60 Sekunden aktualisiert, um Sie auf dem neuesten Stand zu halten.

Mit dem konfigurierten **Admin-Passwort**  ist es möglich, auf eine erweiterte Version der Lizenzüberwachung zuzugreifen, die die neuesten Protokollmeldungen, die Konfigurationseinstellungen und einen Schnitt zur Visualisierung des Checkout-Verlaufs in Diagrammen enthält. Diese Karteikarten werden nicht automatisch nachgeladen.

Bei Bedarf kann der Zugriff auf die grundlegende Lizenzüberwachung vollständig eingeschränkt werden, indem Sie ein **Hauptpasswort**  festlegen.

Checkout-Verlauf

Der VS-Lizenzmanager speichert Daten darüber, wie viele Funktionen im Laufe der Zeit und von welchen Benutzern genutzt werden. Zusätzlich zur Echtzeit-Ansicht der Funktionsnutzung des aktuellen Tages gibt es vorkonfigurierte Diagramme zur stündlichen Nutzung der letzten 24 Stunden, zur täglichen Nutzung der letzten 30 Tage, zur monatlichen Nutzung der letzten 12 Monate und zu den täglich verweigerten Benutzern der letzten 30 Tage. Es ist auch möglich, benutzerdefinierte Diagramme für einzelne Zeiträume zu erstellen.

Die Verwendungsdaten werden im Installationsverzeichnis unter `/data/History/` gespeichert. Die Daten werden im CSV-Format gespeichert und können problemlos für weitere Analysen verwendet werden. Die Spalten sind `time` (Sekunden seit 01.01.1970), `count`, `feature`, `username` und `errorcode`.



Kapitel V:

Fehlerbehebung

5 Fehlerbehebung

„No allow rule found in windows firewall for tcp <port>, license checkout might not be accessible“

- Überprüfen Sie, ob Sie die **konfigurierten Ports in Ihrer Firewall** freigegeben sind.
- Wenn Sie eine Firewall eines Drittanbieters (oder gar keine Firewall) verwenden, können Sie diese Meldung ignorieren. Wir können dies nur erfolgreich überprüfen, wenn die Windows-Firewall aktiv ist.