

CIS Agent

Integrationsagent

Innehållsförteckning

1	twodays integrationstjänst	3
1.1	twodays laaS-plattform.....	3
1.2	Integrationsagenter	4
1.3	Före installation	6
1.4	Installation.....	6
1.4.1	setup_agent.cmd	7
1.5	Avinstallation.....	7
1.6	Kryptering.....	8
1.7	Administration	9
1.8	Nedlåsning av installationen.....	10
1.9	Kommunikation.....	11
1.10	Tidsstyrning	12

1 twodays integrationstjänst

Integration as a Service (IaaS) är en leveransmodell som hanterar systemintegration som en tjänst i molnet. Integrationstjänsten hanterar datatransport mellan kundernas verksamhetssystem och med tredje part (leverantörer och affärspartners). Alla typer av kunder kan använda IaaS därför att arkitekturen möjliggör integration till låg kostnad och med liten påverkan av befintlig IT-miljö. Det innebär att kunderna kan fokusera på sin kärnverksamhet istället för att hantera kostsamma integrationslösningar.

Fördelarna med IaaS:

- Lägre total kostnad p.g.a. lägre investeringskostnad och lägre kostnad för underhåll.
- Kortare leveranstider och fullt skalbara on-demand lösningar gör det möjligt att välja integrationstjänster baserade på föränderliga affärsbehov.
- En hög grad av repeterbara värdeadderade tjänster resulterar i snabbare återbetalning av investeringen.

1.1 twodays IaaS-plattform

Verksamhetssystemen flyttas i allt högre grad till molnet. Det skapar en utmaning i form av att möta verksamhetens behov av applikationsintegration, automatisering av affärsprocesser och datasynkronisering mellan lokala IT-system och applikationer i molnet. twodays integrationstjänst ger kunden tillgång till en uppsättning molntjänster som stöder aktuella behov av systemintegration, både i molnet och i den lokala miljön.

Inom de flesta företag och myndigheter är integrationsplattformen en central del i IT-miljön, eftersom den binder samman interna verksamhetssystem och även hanterar datautbyte med externa IT-system hos leverantörer och andra affärspartners. För att verksamhetsprocesserna ska fungera problemfritt dygnet runt krävs stabila och driftsäkra integrationslösningar.

Med twodays IaaS-plattform kan molntjänstmodellen realiserars även för lokala systemintegrationer. Integrationstjänsten innebär flexibilitet i kombination med enkel och driftsäker hantering. Processerna kan snabbt anpassas efter det aktuella verksamhetsbehovet.

twodays IaaS-lösning är baserad på en teknisk plattform som kan hantera alla typer av integrationsflöden. Integrationsprocesser kan utvecklas, anpassas, driftsättas och övervakas utan minsta ansvar och arbetsinsats för kunden. Med twodays integrationstjänst blir hanteringen av integrationer enkel och problemfri. Ingen hänsyn behöver tas till val och inköp av programvara och teknisk plattform. twoday tar hela ansvaret för utveckling, underhåll och övervakning av integrationsprocesserna som hanteras enligt effektiva metoder och standards.

twodays IaaS-lösning är plattformsoberoende. Alla typer av integrationslösningar kan implementeras. Integrationsflöden kan sättas upp mellan lokala system, mellan system i molnet eller mellan molnsystem och lokala system. twoday IaaS-miljö kan hantera åtkomst till applikationer och data med aktuella standardmetoder som exempelvis REST, JSON, SOAP, XML, CSV, FTP, system-API och filsystem.

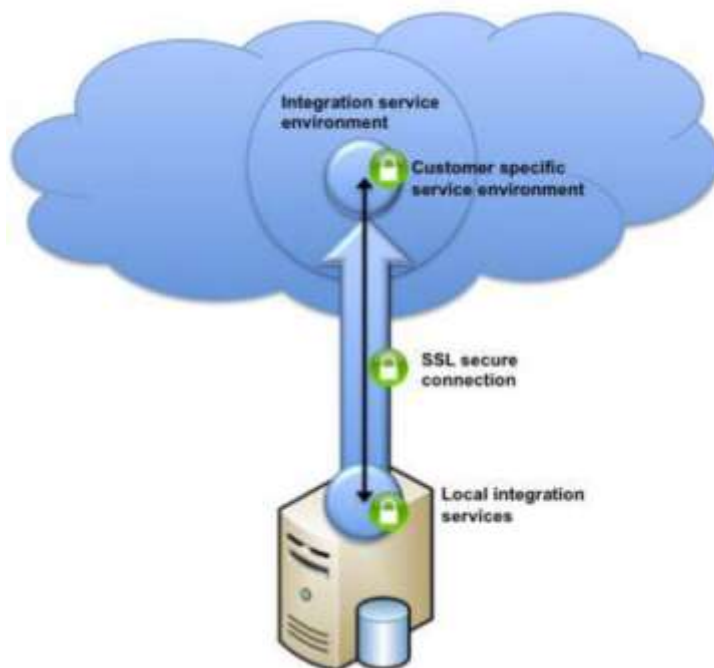
1.2 Integrationsagenter

twodays IaaS-miljö är byggd på en distribuerad arkitektur där den centrala servermiljön innehåller den integrationslogik som ska utföras i kundernas miljöer. IaaS-miljön behöver dock lokal programvara som den kan kommunicera med, så kallade integrationsagenter. Integrationsagenterna arbetar styrda av twodays integrationsserver, deras uppgift är att starta upp och övervaka de processer som servern tilldelar dem.

twodays IaaS server-agent-arkitektur ger gränslösa möjligheter till skalbarhet och lastbalansering. Finns behov av mer prestanda kan fler agenter installeras. Den inbyggda failover-logiken ger en maximal driftsäkerhet, faller en agent bort kan en annan ta över.

Agenterna är plattformsoberoende, de kan både installeras i Windows- och Unix/Linux-miljöer.

När det gäller att hantera integration i molnet är säkerheten en kritisk faktor. Det gäller att säkerställa att varje kunds miljö i molnet är separerad från andra miljöer. Det gäller att säkerställa att datatransport mellan IaaS-miljön och den lokala IT-miljön sker på ett 100% igt säkert sätt. I detta fall gäller det både kommunikationssäkerhet och skydd mot otilbörlig åtkomst. Det gäller också att säkerställa att de lokala integrationsprocesserna inte har åtkomst till data och miljöer utan för det område som integrationen omfattar samt att integrationslogiken inte kan saboteras eller manipulera



All kommunikation mellan den lokala miljön och tjänstemiljön sker i en riktning – den lokala integrationsmiljön (integrationsagenten) kopplar upp sessionen med integrationstjänsten. Det innebär att aktuella brandväggar bara behöver öppnas upp för trafik i utgående riktning mot en given port. När sessionen kopplats upp kan tjänsten styra och övervaka de lokala integrationsprocesserna. Kontroll av agenternas status sker kontinuerligt, skulle någon agent p.g.a kommunikationsproblem inte kunna koppla upp sig upptäcker servern att den "tappat" agenten och ett larm genereras.

Varje enskild kunds integrationsprocesser installeras och exekveras i en separat arbetsarea utan åtkomst till andra delar i integrationstjänsten.

Datautbytet mellan den lokala miljön och integrationstjänsten i molnet sker via en TLS/SSL-krypterad session. Om det finns behov av kryptering och signering på datanivå, kan den funktionen läggas till i processflödet.

Integrationsagenten exekveras som en tjänst (service) kopplad till en viss användarbehörighet. Genom att styra aktuellt användarkontos behörighet till systemmiljön kan risken för otillbörlig åtkomst elimineras.

Integrationsprocesserna levereras som komponenter med öppen källkod, vid behov kan kunden granska och analysera alla detaljer i integrationsprocessen. Det går inte att

manipulera källkoden i komponenterna eftersom de kontrolleras av tjänsten vid exekvering. Om en komponent modifierats lokalt ersätts den av den giltiga komponenten lagrad i molnet innan nästa exekvering.

1.3 Före installation

Integrationsagenten kan installeras på en ordinär Windows eller Linux server. Det finns inga specifika krav på miljön, alla nödvändiga komponenter ingår i installationspaketet. Dock måste brandväggsöppning göras för utgående trafik via port 443, agenten måste kunna nå den integrationsserver som ska styra den.

Agenten exekveras som en tjänst, vilken har ett användarkonto knutet till sig. Detta användarkonto bör ha en lämplig behörighetsnivå, vilken tillåter access till aktuella systems integrationsgränssnitt.

1.4 Installation

twoday tillhandahåller installationsmedia som zip-fil eller msi-paket. Följande länk kan användas för att ladda ner msi-paketet,

<https://delivery.ciceron.cloud/Integration%20Services/win/cis-agent-2.7.14.msi>

Notera! Länken är skyddad och kräver en användare och lösenord. Användaren som kan användas är *delivery*. Lösenordet skickas separat till installatör via SMS.

msi-paketet innehåller en zip-fil för installation av integrationsagenten och kommer att packa upp filer och sen köra `setut_agent.cmd`.

Notera! msi-installationen kommer inte lyckas om något går fel vid installationen. Vid en installation har twoday följande rekommendationer

1. Svara Y till frågan *Edit configuration\setup_agent.txt?* [Y,n]
2. Notepad visar då filen `setup_agent.txt`
3. Sök efter `is_server_address` och sätt det korrekta värdet för test eller produktionsmiljön i.e. `cis-server-test.siriusit.net` eller `cis-server.siriusit.net`
4. Spara filen
5. Svara Y till frågan *Continue with this setup?* [Y,n]
6. Kör inte någon kommunikationstest genom att svara N på frågan *Run communication test?* [Y,N]
7. Windows installer kommer därefter visa en dialog om att installationen är klar

Behöver man nu ändra någon konfiguration så kan man köra scriptet `setup_agent.cmd` igen och ändra inställningar.

1.4.1 setup_agent.cmd

Detta script används för att konfigurera en integrationsagent som körs i aktuell maskin. När setup startar så kommer befintliga inställningar visas för ändring. Inställningarna är endast några miljövariabler som setup använder för att hantera konfiguration. Sen installeras integrationsagenten som en tjänst i Windows.

Den information som är obligatorisk att ange är

- `set is_server_address=`
Anger adressen (host:port) till integrationstjänsten
Standardport är 443 för SSL/TLS kommunikation
- `set is_agent_workspace_id=`
Anger identitet till kundens installation i integrationstjänsten
- `set is_agent_enable_ssl=yes`
`set is_agent_cert_file=keystore\cis_clientcert.p12`
`set is_agent_cert_password=xxxxxx`
Anger information om klientcertifikat som används av kunden. Detta klientcertifikat tillhandahålls av twodays support.

1.5 Avinstallation

Installationen av integrationsagenten återfinns i Windows Control Panel | Programs.

Välj avinstallera och följ sedan instruktionerna.

1.6 Kryptering

Parametrar och konfiguration kan lagras krypterat för integrationsagenten om det finns en krypteringsnyckel. Information om krypteringsnyckel registreras i filen *is_agent.conf* under sektionen *encryption* enligt

```
<pki>
  <!-- inserted somewhere as a child to the pki node -->
  <encryption>
    <key>b0XcGWkxKaQY5pBdN2IJ</key>
  </encryption>
</pki>
```

Notera! Använd en säker lösenords generator för att skapa krypteringsnyckeln

Krypteringsnyckeln kan också lagras i separat fil enligt

```
<pki>
  <!-- inserted somewhere as a child to the pki node -->
  <encryption>
    <key_file>/etc/vault/cis-enc.key</key_file>
  </encryption>
</pki>
```

Integrationsagenten kan därefter kryptera information med hjälp av kommandot

```
is_agent -encrypt "this will be encrypted and used by the agent" -key b6BTvQw4FvVM6qnX
```

Notera! Om man inte anger krypteringsnyckeln ovan så används den konfigurerade krypteringsnyckeln i *is_agent.conf*.

Det finns även möjlighet att kryptera värdet av krypteringsnyckeln. I detta fall krävs att *<key>* och *<key_file>* måste vara konfigurerad enligt

```
<pki>
  <!-- inserted somewhere as a child to the pki node -->
  <encryption>
    <!-- this key was used to create the encrypted content of the key file -->
    <key>b0XcGWkxKaQY5pBdN2IJ</key>
    <!-- this file contains the encrypted value of the real encryption key -->
    <key_file>/etc/vault/cis-enc.key</key_file>
  </encryption>
</pki>
```

Notera! Om krypteringsnyckeln försvinner eller förändras så finns inte möjligheten att dekryptera informationen som lagras krypterat.

Kryptering av information bör användas för konfiguration av lösenordet till klientcertifikatet som används för kommunikation mot integrationstjänsten enligt

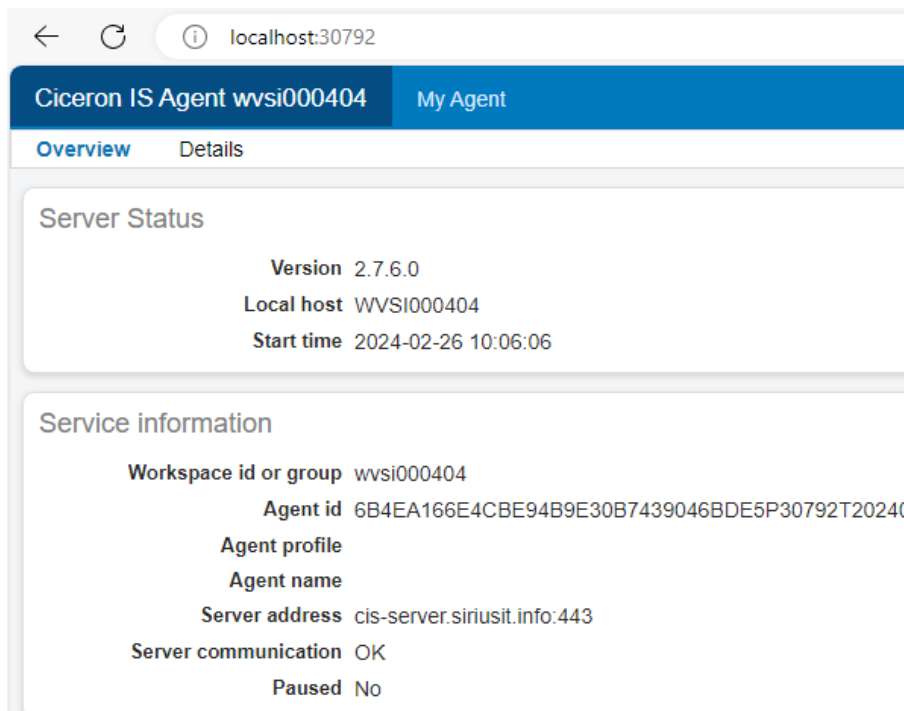
```
<pki>
  <keystore>
    <password>$CIS_VAULT;1.0;AES256;C4D8636BFCF3D68D6051B89F265A85AC.F783193E1484AC8C83
1C82A9AC59B1D0</password>
  </keystore>
</pki>
```

1.7 Administration

Det finns möjlighet att surfa till integrationsagenten efter en installation är genomförd. Som standard används porten 30792 och länken enligt <http://localhost:30792>.

I en standardinstallation krävs en inloggning med en lokal användare på servern där integrationsagenten blev installerad.

För en behörig användare visas följande webbsida med information om installationen



The screenshot shows a web browser window with the URL localhost:30792. The page title is "Ciceron IS Agent wvsi000404" and the user is logged in as "My Agent". The page has two tabs: "Overview" (selected) and "Details".

Server Status

- Version 2.7.6.0
- Local host WWSI000404
- Start time 2024-02-26 10:06:06

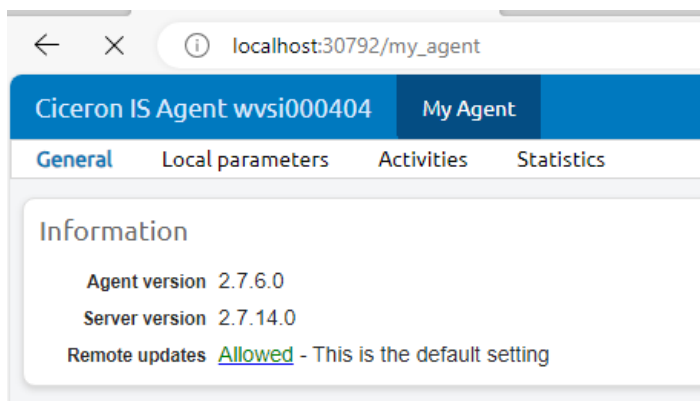
Service information

- Workspace id or group wvsi000404
- Agent id 6B4EA166E4CBE94B9E30B7439046BDE5P30792T20240:
- Agent profile
- Agent name
- Server address cis-server.siriusit.info:443
- Server communication OK
- Paused No

1.8 Nedlåsning av installationen

I en standardinstallation så hämtar integrationsagenten uppdaterade script för integrationen från integrationstjänsten.

Det finns möjlighet att förhindra detta genom att låsa ner installationen. Funktion för detta återfinns under administrationssidorna för integrationsagenten under menyn *My Agent* enligt

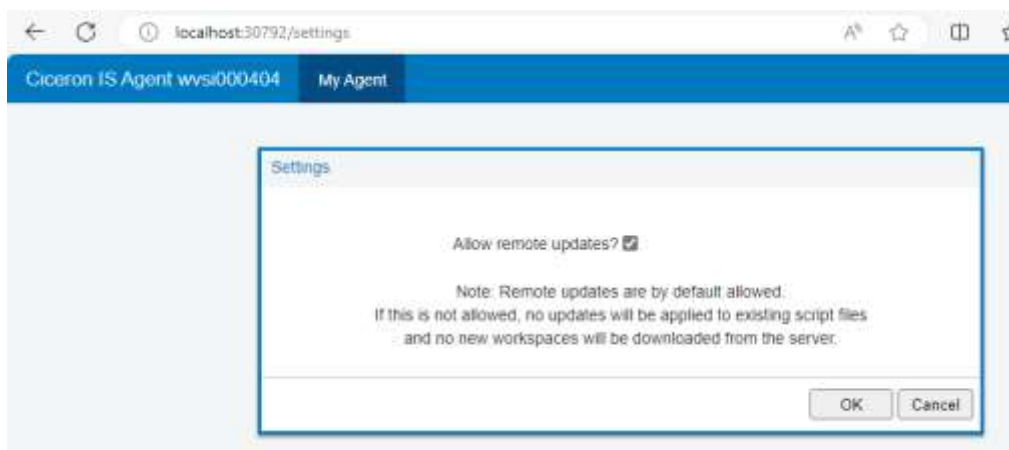


The screenshot shows the "My Agent" page with the "Information" tab selected. The page title is "Ciceron IS Agent wvsi000404" and the user is logged in as "My Agent". The page has four tabs: "General" (selected), "Local parameters", "Activities", and "Statistics".

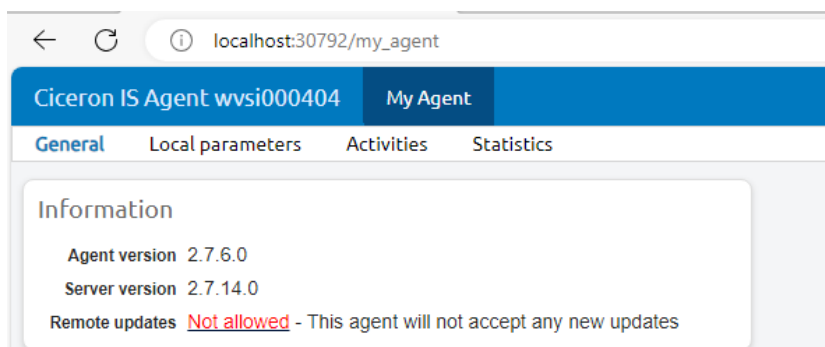
Information

- Agent version 2.7.6.0
- Server version 2.7.14.0
- Remote updates [Allowed](#) - This is the default setting

Genom att klicka på länken *Allowed* så kan man låsa ner installationen. Följande information visas



Genom att ta bort krysset i *Allow remote updates* och därefter klicka på knappen *OK* så låsas installationen ner och följande information presenteras.



Notera! När denna konfiguration är satt så kan inte nya versioner av integrationer levereras till integrationsagenten. Detta innebär att twoday behöver vara i kontakt med personal hos kund när ny version ska levereras.

1.9 Kommunikation

Integrationsagenten anropar integrationstjänsten kontinuerligt för att erhålla information om det finns en integration som ska köras. Detta anrop kan använda kommunikation över

- mTLS med TCP
- UDP

När integrationsagenten använder UDP så skickas ett meddelande till integrationstjänsten med det unika id:et för agenten. Brandväggar med NAT-funktionalitet och de routrarna som finns på kommunikationsvägen till integrationstjänsten kommer då att hålla den initierade kommunikationskanalen öppen under en viss tid (ungefär en minut) och under denna period

kan integrationstjänsten också skicka ett UDP-meddelande tillbaka till integrationsagenten. Meddelandet som skickas tillbaka är endast information om det finns en integration som ska köras eller inte. Finns det en integration som ska köras av integrationsagenten så kopplar den upp sig med mTLS över TCP för att hämta information från integrationstjänsten som krävs för att köra integrationen. Mer information om hur UDP kommunikationen hanteras finns här, [UDP hole punching - Wikipedia](#).

Kommunikationen med UDP såväl som mTLS över TCP använder samma serveradress till integrationstjänsten.

1.10 Tidsstyrning

Det finns även möjlighet att konfigurera att integrationer ska schemaläggas d.v.s. att en integration endast startar vissa tider. Exempel på hur en integration ska schemaläggas är

- Ska köras varje hel timme, varje vardag
- Ska köra 1 gång i månaden

Integrationsagenten får informationen från integrationstjänsten när integrationen ska köras och gör då en uppkoppling med mTLS över TCP. Från integrationstjänsten får då integrationsagenten den information som är aktuell för att köra integrationen.