

# Certificazione di un Resource Provider

## Table of contents

Table of contents .....	1
Document log .....	1
Descrizione del processo .....	1
Procedura di certificazione .....	2
Documenti referenziati .....	3

## Document log

Date	Comment	Authors
2021 Feb 1-5	Review on General	Salomoni D.
2021 Jan 29	Discussion on WP4	Duma D.C., Sgaravatto M., Veraldi R., Traldi S., Antonacci M., Stalio S., Ciaschini V., Spinoso V.
2020 Apr 17	First draft	Spinoso V., Duma D. C., Traldi S.
2020 Dec 14	Beta	Spinoso V.

## Descrizione del processo

Quando un Resource Provider chiede di entrare nella federazione, esso accetta le Rules of Participation di INFN Cloud, e, in particolare, accetta di superare il processo di certificazione.

Il processo di certificazione di un Resource Provider ha l'obiettivo generale di validare operativamente un Resource Provider durante la procedura di onboarding nella federazione di INFN Cloud. Il superamento del processo di certificazione rappresenta condizione necessaria per l'integrazione nella federazione di INFN Cloud.

Obiettivo complessivo del processo è accertare che un Resource Provider risponda a un set di requisiti minimi come specificato dalle Rules of Participation per potersi federare. Esso deve infatti:

- soddisfare tutte le caratteristiche richieste dalla federazione
- dimostrare di essere in grado di sostenere le richieste minime complessive (in termini sia di risorse che di supporto) come definito dal Management Board di INFN-Cloud

Operativamente, il processo consiste in una serie di passi da eseguire e di test da superare da parte del Resource Provider insieme con il team di Operations di INFN Cloud.

Il processo di certificazione include requisiti minimi, verificati attraverso:

- controlli automatici (effettuati attraverso opportune "probe" software)
- verifiche operative dirette da parte del team di certificazione ("Operations").

Il processo di certificazione comincia in una specifica data concordata tra il team di certificazione e il Resource Provider candidato e termina dopo al massimo 60 giorni; se entro tale periodo, a valle del lavoro

congiunto dell'amministratore del sito e del Team di INFN Cloud il sito non viene certificato, INFN Cloud può valutare di non certificare il sito o di sospendere il processo di certificazione, per riprenderlo eventualmente quando cambiano le condizioni che hanno determinato la sospensione.

Il processo di certificazione si svolge interamente attraverso il sistema Service Desk di INFN Cloud, cominciando nel momento in cui il Resource Provider apre il ticket a INFN Cloud per richiedere la certificazione.

Il Resource Provider può essere integrato in INFN Cloud quando i seguenti requisiti sono entrambi verificati:

- tutti i passi della procedura più sotto descritta sono stati eseguiti
- tutti i test rimangono superati per 15 giorni successivi

## Procedura di certificazione

### Nomenclatura

- Resource Provider: identifica il proprio Cloud team certificatore
- Operations: identifica il team INFN Cloud di supporto alla certificazione

Step #	Responsabile	Azione
1	Resource Provider	<p>Aprire ticket a Operations su Service Desk, richiedendo al team di Operations di definire:</p> <ul style="list-style-type: none"> <li>• ID del Resource Provider (es. INFN-CNAF)</li> <li>• nome del Resource Provider (es. CNAF)</li> </ul> <p>Nel ticket, il Resource provider dovrà fornire le seguenti informazioni:</p> <ul style="list-style-type: none"> <li>• e-mail per comunicazioni generali</li> <li>• e-mail per comunicazioni di sicurezza</li> <li>• e-mail per comunicazioni di emergenza (deve essere necessariamente diverso dai primi due, e in caso questi due non funzionino)</li> <li>• numero di telefono per comunicazioni generali</li> <li>• numero di telefono per comunicazioni di sicurezza</li> <li>• numero di telefono per comunicazioni di emergenza (deve essere necessariamente diverso dai primi due, e in caso questi due non funzionino)</li> <li>• latitudine e longitudine</li> </ul> <p>È richiesta, inoltre, una breve descrizione qualitativa dei seguenti aspetti:</p> <ul style="list-style-type: none"> <li>• informazioni generali sul setup del cloud framework da federare (nome e versione del framework, nome e versione del sistema operativo utilizzato)</li> <li>• processo di aggiornamento del sistema operativo e del framework, con particolare riferimento agli aggiornamenti di sicurezza</li> <li>• separazione tra il traffico di rete relativo al servizio e quello relativo alla gestione dell'infrastruttura</li> <li>• processo di gestione dei log</li> </ul>

		<ul style="list-style-type: none"> <li>• processo di nomina di amministratore dei servizi cloud, a quali componenti dell'infrastruttura ha accesso</li> <li>• se i servizi cloud girano su sistemi dedicati o condivisi</li> <li>• se sono abilitati altri utenti oltre a quelli di INFN Cloud</li> <li>• processo di sospensione di un utente o di un gruppo di utenti, con particolare riferimento alle VM running</li> </ul>
2	Operations	<ol style="list-style-type: none"> <li>1. Verifica le informazioni fornite dal Resource Provider (ad esempio, Operations può mandare dei messaggi di test ai contatti forniti per verificare che venga data risposta)</li> <li>2. Invia al Resource Provider le guide per: <ul style="list-style-type: none"> <li>• l'integrazione con l'infrastruttura di INFN Cloud</li> <li>• l'installazione e configurazione dei servizi abilitanti lato Resource Provider</li> </ul> </li> </ol>
3	Resource Provider + Operations	<ul style="list-style-type: none"> <li>• Il Resource Provider provvede all'integrazione del sito seguendo le istruzioni fornite, interagendo con il team di Operations</li> <li>• Il team di Operations completa la configurazione del sito sui servizi centrali, in particolare per quanto riguarda: <ul style="list-style-type: none"> <li>○ Monitoring</li> <li>○ Accounting</li> <li>○ SLAM/CMDB e Orchestratore</li> </ul> </li> </ul>
4	Operations	<ul style="list-style-type: none"> <li>• Effettua i test manuali (script di validazione)</li> </ul>
5	Operations	<ul style="list-style-type: none"> <li>• Verifica che i controlli automatici siano OK per 15 giorni consecutivi</li> <li>• Se nell'ambito di 60 giorni dall'apertura del ticket il sito non risulta ancora certificato, Operations può valutare di non certificare il sito o di sospendere il processo di certificazione, per riprenderlo eventualmente quando cambiano le condizioni che hanno determinato la sospensione.</li> <li>• Nel caso in cui tutti i test eseguiti, sia automatici che manuali, siano validi, il team di Operations fornisce nel ticket un summary report relativo ai test svolti. Dichiarando quindi il sito certificato e chiude il ticket.</li> </ul>

## Documenti referenziati

- Guida di installazione e configurazione dei servizi abilitanti per il Resource Provider (per i Resource Provider admin)
- Rules of Participation